ORDER FOR SUPPLIES AND SERVICES

REQUISITION/REFERENCE NUMBER	PAGE	OF	PAGES
000000K4	1		4

1. DATE OF ORDER	2. ORDER NUMBER	3. CONTRACT NUMBER	4. PDN NUMBER
09/24/2021 03:05:11 PM EDT	47QFRA21F0038	47QRAD20DU109	

FOR GOVERNMENT USE ONLY

5. ACCOUNTING AND APPROPRIATION DATA

FUND	FUNCTION CODE	B/A CODE	CC-A	C/E CODE	FY	REGION
285F	AF151	AA20		H08		
CC-B	**PROJ./PROS NO.**	**O/C CODE**	**ORG. CODE**	**W/ITEM**	**PRT./CRFT**	
		25	Q08FA000			

6. TO: CONTRACTOR (Name, address and zip code)

MIRACLE SYSTEMS LLC 1621 N KENT STREET SUITE 1000 ARLINGTON, Virginia 22209-2141 United States 571-331-1355

7. TYPE OF ORDER

A. ☐ PURCHASE

Please furnish the following on the terms and conditions specified on the order and the attached sheets, if any, including delivery as indicated.

B. ☐ DELIVERY (For Supplies)

This delivery order is issued subject to the terms and conditions of the above numbered contract.

C. ☒ TASK ORDER (For Services)

This task order is issued subject to the terms and conditions of the above numbered contract.

8A. Data Universal Numbering System (DUNS) Number	8B. Taxpayer Identification Number (TIN)
133239397	(b) (6)

9A. BUSINESS CLASSIFICATION

Limited Liability Company

D. MODIFICATION NUMBER	AUTHORITY FOR ISSUING
P00000	

Except as provided herein, all terms and conditions of the original order, as heretofore mentioned, remain unchanged.

9B. START DATE: 09/27/2021

9C. COMPLETION DATE: 09/26/2022

10. ISSUING OFFICE (Address, Zip Code, and Telephone Number)

Denver Federal Center W 6th Avenue & Kipling Street Denver, Colorado 80225 United States Jessica L Conway-Ellis (b) (6) jessica.conway-ellis@gsa.gov

11. REMITTANCE ADDRESS (MANDATORY)

MIRACLE SYSTEMS LLC 26016 RACHEL HILL DR Arlington, Virginia 22209-0000 United States

12. SHIP TO (Consignee Address, Zip Code and Telephone Number)

National Protection & Programs Directorate Colleen A McDarby 1401 South Clark Street Arlington, Virginia 22202-0000 United States 202-878-2765

13. PLACE OF INSPECTION AND ACCEPTANCE

Colleen A McDarby 1616 North Fort Myer Drive Arlington, Virginia 22202-0000 United States 202-878-2765

14. REQUISITION OFFICE (Name, Symbol and Telephone Number)

GSA FAS AAS Region 08 Denver Federal Center W 6th Avenue & Kipling Street Denver, Colorado 80225 United States Diana E Zoppi (b) (6) diana.zoppi@gsa.gov

15. F.O.B. POINT	16. GOVERNMENT B/L NUMBER	17. DELIVERY F.O.B. POINT	18. PAYMENT/DISCOUNT TERMS
Destination		09/26/2022	Net 30 Days / 0% 0 Days

19. SCHEDULE

ITEM NUMBER (A)	SUPPLIES OR SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	See Continuation Page				

20. RECEIVING OFFICE (Name, Symbol and Telephone Number)

National Protection & Programs Directorate (202) 603-3769

TOTAL FROM 300-A(s)

21. MAIL INVOICE TO: (Electronic Invoice Preferred)

General Services Administration (FUND)
The contractor shall submit invoices electronically by logging into the ASSIST portal (https://portal.fas.gsa.gov),navigating to the appropriate award, and creating the invoice for that award. For additional assistance contact the ASSIST Helpdesk at 877-472-4877. Do NOT submit any invoices directly to the GSA Finance Center (neither by mail nor via electronic submission).

22. GROSS SHIP WEIGHT

GRAND TOTAL $23,923,278.94

23. SHIPPING POINT

See Block 6

24A. FOR INQUIRIES REGARDING PAYMENT CONTACT: KC Finance Accounts Payable

24B. TELEPHONE NUMBER 1-800-676-3690

25A. NAME AND TITLE OF OFFEROR/CONTRACTOR

Sandesh Sharda

26A. UNITED STATES OF AMERICA *(NAME OF CONTRACTING/ORDERING OFFICER)*

David J Shamburger

25B. SIGNATURE	25C. DATE SIGNED	26B. SIGNATURE	26C. DATE SIGNED
Sandesh Sharda	09/24/2021 03:03:23 PM EDT	David J Shamburger	09/24/2021 03:05:11 PM EDT

Program Management Support Services

Performance Work Statement (PWS)

1.0 PURPOSE

The purpose of this Task Order is to provide the Cybersecurity and Infrastructure Security Agency (CISA) with professional services essential to the daily operation and execution of programs and priorities leading to the Cyber Security Directorate's mission success. Program management support services include a full range of management and consulting professional services to meet mission goals and improve agency performance including project management, program acquisition support, business process management, administrative and knowledge management, budget and financial management, communications management and outreach, governance and policy, and order management.

2.0 BACKGROUND

The Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) is responsible for enhancing the security, resiliency, and reliability of the nation's cyber and communications infrastructure. CISA actively engages the public and private sectors as well as international partners to prepare for, prevent, and respond to catastrophic incidents that could degrade or overwhelm these strategic assets.

CISA partners with industry and government to understand and manage risk to our Nation's critical infrastructure. CISA works to prevent or minimize disruptions to our critical information infrastructure to protect the public, economy, government services, and the overall security of the United States. It does this by supporting a series of continuous efforts designed to further safeguard federal government systems by reducing potential vulnerabilities, protecting against cyber and physical intrusions, and anticipating future threats.

Within CISA, the Cybersecurity Division (CSD) leads efforts to protect the federal ".gov" domain of civilian government networks and to collaborate with the private sector - the ".com" domain - to increase the security of critical networks. The CSD mission is to understand evolving threat activity as it affects national critical functions and high value assets, ensuring stakeholder access to essential data on the risk posture of key information systems. This is achieved by using sensors and data feeds which permit CSD to manage and assess relevant incidents and report this threat activity to our stakeholder partners. Once detected, CSD will delay, disrupt, and/or prevent threats from proliferating across the enterprise by deploying technology designed to reduce the vulnerability to the enterprise. The effectiveness of this strategy is maximized through trusted information sharing partnerships with stakeholders, codified by mutually agreed upon processes and procedures. CSD furthers provides value-added to the cyber ecosystem by analyzing its cyber protection strategy, giving assistance to defeat the gravest threats and vulnerabilities as dictated. Within CSD, Capacity Building (CB) helps stakeholders better manage cybersecurity risk by defining expectations for stakeholder cybersecurity; leading implementation and enforcement of cybersecurity requirements; managing CISA's cybersecurity services portfolio; and building capacity and enhance collective defense/readiness.

This procurement primarily provides support to Capacity Building (CB). However, CB's mission is charged with supporting and partnering with multiple stakeholders across the Civilian Executive Branch (FCEB) as well as continual collaboration within CISA as well as CSD SubDivisions. Support services shall address, as needed, the professional services needs of CB as well as CSD as they are prioritized and evolve over the period of performance.

The below provides an overview of the current CB organization, mission and programs that the identified tasks will primarily support. Note: Over the PoP of this TO it is anticipated that the CB organization will evolve, missions will grow, and priorities will change. The contractor shall be flexible and agile in adjusting to a complex and evolving cybersecurity organization in their ability to effectively and efficiently support change.

2.1 CAPACITY BUILDING MISSION

Capacity Building serves as CISA's enterprise cybersecurity services management arm for national stakeholders and the lead for federal enterprise cybersecurity governance. CB enables its customers to manage cybersecurity risk by building their capacity to implement effective cybersecurity policies, tools, and procedures. CB helps stakeholders better manage cybersecurity risk by defining expectations for stakeholder cybersecurity; leading implementation and enforcement of cybersecurity requirements; managing CISA's cybersecurity services portfolio; building capacity; and enhancing collective defense and readiness. Specifically, CB enhances stakeholder cybersecurity readiness, bolsters enterprise capabilities and protections, and increases the community's capacity to adequately manage cyber risk by:

- Defining critical requirements, needs, and performance expectations.
- Overseeing and guiding the implementation of key cybersecurity initiatives and urgent actions, including federal cybersecurity policy, leading practices, cyber directives and operational guidance.
- Managing CISA's cybersecurity services portfolio; evolving shared services, capabilities and delivery models; and delivering tailored services and assistance based on customer needs.

Within CB, there are currently seven (7) branches: Business Operations, Acquisition and Budget (AB), the Continuous Diagnostics and Mitigation (CDM) Program, Customer Experience (CX), Cyber Quality Service Management Office (QSMO), Cyber Threat Information Sharing (CTIS), and Enterprise Implementation (EI) (EI Branch consists of: Standards and Engineering, High Value Assets (HVAs), Directives and Governance, Cyberstat and FISMA).

Provisioning critical, enterprise-wide cybersecurity services and programs is a critical component of CISA's mission to ensure the security of federal networks. Maturity in cybersecurity varies by agency with Federal government facing common, significant challenges in securing information technology from cybersecurity risk. In April of 2019, OMB released a memo offering guidance to address some of these challenges and risks. OMB pre-designated CISA as the Cyber Quality Service Management Office (QSMO). CISA's Cyber QSMO will be a government marketplace of high-quality cybersecurity services that align with federal requirements in a cost-effective manner. The QSMO is responsible for offering solutions for common technology or fully managed services. QSMO must ensure these solutions are cost-effective and sustainable while offering increased efficiencies and enhanced security throughout the FCEB.

2.1.1 BUSINESS OPERATIONS

The Business Operations Team's mission and purpose is to provide quality customer services and mission support to CB while establishing effective solutions to improve business processes and operations. Business Operations leads efforts to enhance CB business lines of service by:

- Performing traditional administrative roles and responsibilities in the areas of Human Capital, Workforce Operations, Employee Engagement, Executive Secretariat (ExecSec), Facilities, and Information Management.
- Serving as the CB Portfolio Management Office (PfMO) responsible for managing and coordinating cross-CB and CSD Cyber Programs, projects, and priorities to ensure efficient and effective management and reporting of our efforts.

2.1.2 ACQUISITION AND BUDGET

AB leads the following efforts:

- Collaborating with stakeholders to gather requirements and develop, manage, and oversee unique and complex acquisition strategies, for cybersecurity capabilities to provide commercial offerings to the .Gov enterprise, as well as SLTT entities
- Providing pre- and post- award contract management
- Tracking CB's Contractor Manpower and Security.
- Managing and executing tool procurements/maintenances.
- Managing vendor relationships, performance and industry communications.
- Performing budget and financial management including all formulation, execution, and cost activities.

2.1.3 CONTINUOUS DIAGNOSTICS AND MITIGATION (CDM) PROGRAM

The CDM Program is responsible for enhancing the security, resilience, and reliability of the Nation's cyber and communications infrastructure. The CDM Program mission is to safeguard and secure cyberspace in an environment where the threat of cyber-attack is continuously growing and evolving. The CDM Program defends the United States (U.S.) Federal IT networks from cybersecurity threats by providing continuous monitoring sensors (tools), diagnosis, mitigation tools, and associated services to strengthen the security posture of Government networks. The CDM Program provides cybersecurity tools, integration services, and dashboards to participating agencies to support them in improving their respective security postures. Program objectives are to reduce agency threat surface, increase visibility into the federal cybersecurity posture, improve federal cybersecurity response capabilities, and streamline Federal Information Security Modernization Act (FISMA) reporting.

2.1.4 CYBER TREAT INFORMATION SHARING (CTIS)

Cyber Threat Information Sharing (CTIS) is working to establish a National Cyber Threat Information Sharing Enterprise (a connected automated machine-to-machine connected community of Federal, SLTT, private sector, and international partners). CTIS is dedicated to enhancing cybersecurity through sharing of accurate, actionable, timely, and relevant cyber threat information to enhance the security posture of the computer network defense community.

The CTIS Branch is responsible for managing National cyber threat information sharing efforts to eliminate cyber threats through defining, building, and managing the cyber threat information sharing environment including the following:

- The Automated Indicator Sharing (AIS) capability enables the exchange of cyber threat indicators between the Federal Government, private sector, and international entities at machine speed.

- Enhanced Cybersecurity Services (ECS) is an intrusion detection and prevention capability that is available to U.S.-based public and private entities. CISA partners with service providers that build and maintain classified systems capable of protecting ECS's customer networks against unauthorized access, exploitation, and data exfiltration utilizing classified data.
- Shared Cybersecurity Services (SCS) is a CISA Program that provides no-cost access to commercial threat feeds for Federal Civilian Departments and Agencies (D/As) (including CISA), state fusion centers, Multi-State Information Sharing and Analysis Center (MS-ISAC), Elections Infrastructure – Information Sharing and Analysis Center (EI-ISAC), and election security organizations. SCS offers access to their respective cyber threat intelligence platforms, application programming interfaces, analytical support, and platform tech support/training.

2.1.5 CYBER QUALITY SERVICE MANAGEMENT OFFICE (QSMO)

CISA's Cyber Quality Service Management Office (QSMO) is the single shared service office for managing cybersecurity solutions for the Federal Civilian Executive Branch (FCEB). CISA's Cyber QSMO centralizes, standardizes, automates, and offers high-quality, cost-effective cybersecurity services and products on the Cyber QSMO Marketplace, providing federal civilian departments and agencies with a one stop-shop for cybersecurity services. As part of our end-to-end service management model, the QSMO provides integration and adoption support to customers through a unified shared services platform.

2.1.6 CUSTOMER EXPERIENCE (CX)

The CX Branch collaborates and advises on the execution of customer experience activities by internal programs to help build a customer-centric culture. This is accomplished by:

- Providing pre-launch services guidance to the relevant internal program to support the adoption and implementation of a human-centered design approach to engaging customers in the service development process
- Conducting qualitative, quantitative, and historical research to mine customer insights and understanding
- Supporting post-launch customer engagement to collect feedback
- Leading efforts to standardize the solicitation of feedback from customers to create consistent feedback approaches
- Improving the feedback collection process to ensure it transitions into actionable data.

2.1.7 ENTERPRISE IMPLEMENTATION

Enterprise Implementation demonstrates leadership in cybersecurity risk management by providing targeted guidance and solutions to help FCEB agencies address today's most pressing challenges and to reduce risk. EI strategically leverages knowledge and agency collected information to drive solutions, services, and capabilities to secure federal networks and protect FCEB agencies' missions.

The Branch oversees the operationalization of foundational levels of cybersecurity capabilities across the Federal Civilian Executive Branch (FCEB) Enterprise, aligning defined risk thresholds with effective mechanisms to execute governance and implementation actions. In partnership with OMB, EI integrates planning, governance, and assistance efforts to ensure CISA and the

FCEB are working toward common goals that increase enterprise cybersecurity maturity. Specifically, EI performs the following:

- Identifies agency challenges and validates FCEB priorities through trends analysis and interagency relationship management
- Analyzes and researches issues and priorities to develop FCEB-wide strategic planning and frameworks, programming approaches, policy guidance, and recommendations
- Provides agency oversight and tracks compliance with planning, policy, and guidance actions and provides direct assistance to improve agency accountability
- Identifies the approaches needed to successfully implement the identified recommendations, approaches, and guidance across the FCEB, and serves as the Standards Area Lead
- Identifies, develops and executes functions of the Federal Cybersecurity Risk Administrator (FCRA).

2.1.8 CYBERSECURITY DEFENSE EDUCATION AND TRAINING (CDET)

As the Nation's Risk Advisor, CISA leads the effort to ensure there is an appropriate staffing of cybersecurity professionals to address the increasing demand of protecting the government, critical infrastructures, SLTT, and public/private partners. To accomplish this, CISA is standing up the Cybersecurity Defense Education & Training (CDET) Subdivision to consolidate and expand the agency's ability to address this workforce shortage crisis.

2.2 SCOPE

The scope of this PWS encompasses professional support services across CB, which includes but is not limited to: acquisition support (program level), administrative support (senior/intermediate), budget and financial management, communications management and outreach, governance and policy, project management, human capital and resource management, product management, and pre/post-award contract requirements management. The CB mission and priorities are dynamic and complex and as such the contractor shall use strategic vision, leverage a diverse team of subject matter experts, be flexible in addressing these professional support requirements and be pro-active and capable and ready to surge as requirements evolve. This Task Order (TO) describes the full range of program management services to support CSD's and CB's cybersecurity mission areas.

The primary place(s) of performance at Task Order Award (TOA) is at contractor's facility due to the current circumstances of the national pandemic. See Section 13.0 Contract Telecommuting-Remote Personal Residence Work Locations for additional approved work locations.

During the PoP of the TO and as the workplace circumstances evolve the contractor shall perform the TO requirements on-site at the government's facility located in Ballston, VA and off-site at the contractor facility. An on-site support schedule will be identified post-award. It is preferred that the contractor's facility be within the Washington DC metro area/NCR and near the Government's location in Arlington, VA (Ballston area). The contractor shall be required to routinely travel to the to the Government's location in Arlington, VA (Ballston area). The contractor's facility shall include conference and meeting room space and support routine

Government meetings and events. The contractor shall provide support during normal operating hours from 0800 to 1700 daily, five (5) days a week (Monday through Friday).

2.2.1 CONTRACTOR ROLES AND RESPONSIBILITIES

In addition to the services awarded through this TO, the government will maintain existing contracts and/or award new contracts to support current and future CB requirements. IAW tasks listed in Section 3, the contractor shall support CB in the drafting and/or oversight of these contracts, specifically; drafting of new requirements and solicitation documentation; deliverable control and management, managing internal PMO processes, supporting PMO portfolio teams/section chiefs and senior leaders. As such, the contractor shall be precluded from bidding on any future requirements for which it supported the preparation development of any acquisition documentation.

Additionally, during performance of this TO, the contractor shall be required to work closely with the government team, federal agencies external to DHS and other contractors including CB Support contractors and Federally Funded Research and Development Centers (FFRDCs) to help meet program and/or project objectives. Delineation of contractor roles and responsibilities is critical to the success of the support (please see Section 12.0 for Organizational Conflict of Interest clauses). Figure 2 below provides the current organizational structure of the CB Subdivision. The contractor shall provide support across and through the various verticals within the Subdivision organization.

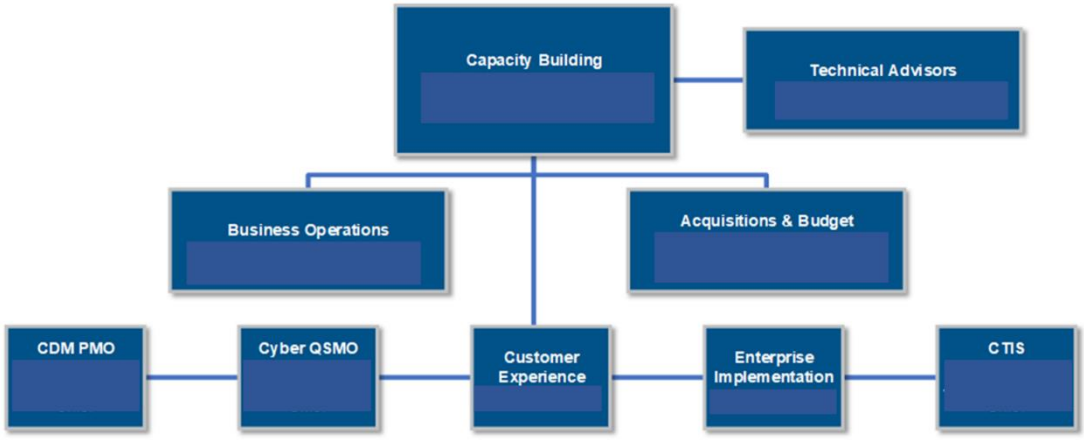

Figure 1: Capacity Building Organizational Structure

3.0 TASKS

The contractor shall provide the support described in the following overarching tasks:

- 3.1 Task 1 – Provide Task Order Project Management and Administration
- 3.2 Task 2 – Provide Project Management Support
- 3.3 Task 3 – Provide Program Acquisition Support
- Expand and/or surge support to 3.3.1 Subtask 3.1 – Provide Program Acquisition Support, 3.3.2 Subtask 3.2 – Provide Program Lifecycle Logistics Support, and 3.3.3 Subtask 3.3 – Provide Quality and Records Management as CB mission and priorities expand and evolve.
- 3.4 Task 4 – Provide Product Management Support
- 3.5 Task 5 – Provide Budget and Financial Management Support
- 3.6 Task 6 – Provide Communications and Outreach Support
- 3.7 Task 7 – Provide Administrative and Knowledge Management Support
- 3.8 Task 8 – Provide Governance and Policy Support

3.9 TASK 9 – PROVIDE PROJECT TRACKING/ORDER MANAGEMENT SUPPORT

Acquisition and Budget (AB) enhances CB subdivisions and its customer agencies by leading full lifecycle acquisition and establishing innovative acquisition solutions. AB fosters partnership and collaboration with industry and customer agencies to lead and deliver complex, large scale cybersecurity acquisitions, budget, and project management activities on behalf of CB. Support includes researching, developing, and managing innovative information technology (IT) acquisition and contract strategies, providing oversight, review, and approval of contract deliverables, and manage contract operations and performance by ensuring contractors deliver high-quality solutions on time, and leading pre-award and post-award acquisition tasks and requirements development to create flexible, fast, and cost-effective vehicles.

-

Associated deliverables with the above Task areas are identified throughout Section 3 and a consolidated list is provided in Section. The tasks are separated into mandatory (tasks not identified as “optional”) and optional. Mandatory Tasks shall be executed at TOA and optional shall be executed throughout the PoP at the direction of the Government. Throughout the PoP the Government fully anticipates the support to grow and fluctuate and the need to surge via the optional tasks to adequately meet and support evolving cybersecurity priorities. As such, the contractor shall be pro-active and plan and manage resources accordingly to meet this dynamic requirement.

3.1 TASK 1 – PROVIDE TASK ORDER PROJECT MANAGEMENT AND ADMINISTRATION

The contractor shall provide project management support under this TO. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified in this PWS. The contractor shall identify a

Project Manager (PM) by name who shall provide management, direction, administration, quality assurance, and leadership of the execution of this TO.

The contractor shall use industry-best standards and proven methodologies that ensure all TO activities are identified, documented, and tracked so that the TO can continuously be evaluated and monitored for timely and quality service. The contractor shall notify the Contracting Officer (CO) and Contracting Officer's Representative (COR) of any technical, financial, personnel, Organizational Conflict of Interest (OCI), or general managerial problems encountered throughout the life of the TO.

The contractor shall facilitate Government and contractor communications and all activities necessary to ensure the accomplishment of timely and effective support, performed in accordance with the requirements contained in this TO.

3.1.1 SUBTASK 1.1 – COORDINATE A PROJECT KICK-OFF MEETING

The contractor shall schedule and coordinate a Project Kick-off Meeting within two (2) weeks after TO award (TOA) in the National Capital Area (NCR) at a location approved by the Government or virtually via Microsoft Teams. The meeting will provide an introduction between the contractor personnel and Government personnel who will be involved with the TO. The meeting will provide the opportunity to discuss technical, management, and logistic issues; travel authorization; and reporting procedures. At a minimum, the attendees shall include key contractor personnel, COR, Functional Leads, key Government representatives, and the Contracting Officer (CO). The contractor shall provide a Kick-Off Meeting Agenda **(Deliverable 1)** that will include, but not limited to, the following:

- Introduction of personnel
- Overview of project tasks
- Overview of organization (complexity)
- Schedule (shows major tasks, milestones, and deliverables; planned and actual start and completion dates for each)
- Communication Plan/lines of communication overview (between both contractor and Government)
- Discussion of draft Program Management Plan (PMP)
- Travel notification and processes
- Government-furnished information (GFI)
- Manpower/staffing status
- Security requirements (Building/LAN-A access, badges, etc.)
- Invoice procedures
- Monthly meeting dates
- Reporting Requirements, e.g. Monthly Status Report (MSR)
- POCs
- Roles and Responsibilities
- Transition-In Plan to include process, timeframes, and status
- Prioritization of contractor activities
- Any initial deliverables

- Other logistic issues
- Quality Control Plan (QCP)
- Sensitivity and protection of information
- Additional issues of concern (Leave/back-up support).

The contractor shall provide a draft copy of the agenda for review and approval by the COR prior to finalizing. The Government will provide the contractor with the number of participants for the kick-off meeting and the contractor shall provide sufficient copies of the presentation for all present **(Deliverable 2).**

3.1.2 SUBTASK 1.2 – PREPARE MANAGEMENT REPORTS

MONTHY STATUS REPORT (MSR) BRIEF

The contractor PM shall develop and deliver a MSR briefing **(Deliverable 3)** using the template provided **(Attachment A – Monthly Status Report Template)** by the tenth (10^{th}) of each month or the following business day (if the 10^{th} falls on a Saturday or Sunday) via electronic mail (email) to the COR**.** The briefing shall briefly summarize, by task, the management and technical work conducted during the month. The contractor shall provide at a minimum the following information:

- Activities during reporting period, by task and subtask to include: On-going activities, new activities, activities completed, deliverables submitted for that period; and progress to date on all above-mentioned activities. Start each section with a brief description of the task.
- Problems and corrective actions taken. Also include issues or concerns that may affect project milestones, personnel, and cost resources and proposed resolutions to address them to include risk mitigation plans.
- Manpower Status - Personnel gains, losses, and staffing status (upcoming leave, security status, etc.) (LH only).
- Government actions required (deliverables awaiting Government approval, etc.).
- Schedule (from the PMP **(Deliverable 8)** shows major tasks, milestones, and deliverables; planned and actual start and completion dates for each).
- Summary of trips taken, conferences attended, etc.
- Projected cost of each CLIN broken-down by Task and Subtask for the current month for tracking purposes.
- Financial status including (LH only):
    - Chart reflecting funding and burn rate for the month and cumulative
    - Cumulative invoiced costs for each CLIN and Labor Tasks totals to-date.
- A list of current deliverables and milestones generated from the PMP identifying deliverable due dates. The list shall identify deliverables and milestones submitted for the period by task as well as provide a projection for the following three (3) months.
- Recommendations for change, modifications, or improvements in task or process.

The contractor shall reconcile the MSR with each monthly invoice.

The contractor shall conduct a Monthly Status Briefing to brief the COR, CISA Functional Leads and other Government resources on the status of the TO and activities. at a location approved by the Government or virtually through Microsoft Teams. The purpose of this meeting is to ensure all stakeholders are informed of the monthly activities and the MSR, provide opportunities to identify other activities and establish priorities, and coordinate resolution of identified problems or opportunities. The contractor shall provide minutes of these meetings, including attendance, issues discussed, decisions made, and action items assigned, to the COR **(Deliverable 4)**.

TRIP REPORTS

The Government will identify the need for a Trip Report (if required) when a request for travel is submitted (see Section 6.0 Travel). The contractor shall submit Trip Reports five (5) working days after completion of a trip for all long-distance travel **(Deliverable 5).**

The Trip Report will include the following information:

- Personnel traveled
- Dates of travel
- Destination(s)
- Purpose of trip
- Cost of the trip
- Approval authority
- Summary of events, action items and deliverables

The contractor shall keep a historical summary of all long-distance travel, to include, at a minimum, the name of the employee, government approval authority, and location of travel, duration of trip, total cost and purpose.

MEETING REPORTS

The Government will identify the need for a Meeting Report (if required) when a meeting is scheduled. The contractor shall submit Meeting Reports to document results of meetings **(Deliverable 4)** one (1) working day following the competition of each meeting. The Meeting Report shall include the following information:

- Meeting attendees and their contact information – at minimum identify organizations represented
- Meeting dates
- Meeting location
- Purpose of meeting
- Summary of events, action items and deliverables

The contractor shall reconcile their Meeting Report with official meeting minutes if published and advise the COR accordingly.

PROBLEM NOTIFICATION REPORTS (PNRS)

The contractor shall file a Problem Notification Report (PNR) one day after the problem is identified **(Deliverable 6)** to notify the COR of TO issues such as potential cost/schedule

overruns/impacts, assumptions upon which tasks were based that have changed or were incorrect, etc. The PNR shall be prepared in accordance with the sample provided and include a plan detailing the proposed resolution.

3.1.3 SUBTASK 1.3 – PREPARE A PROGRAM MANAGEMENT PLAN (PMP)

The contractor shall develop and deliver a Draft and Final PMP **(Deliverable 7 and 8)** that is based on the contractor's proposed approach to the TO. The contractor shall document all support requirements in the PMP. The PMP shall cover the entire project and outline the tasks and deliverables necessary to meet the PWS objectives. The PMP shall include milestones, tasks, and subtasks required in this TO. The contractor shall present and brief the draft PMP at the Kick-Off meeting. Following the Kick-Off meeting, the contractor shall revise the PMP to incorporate Government comments. The PMP shall contain, at a minimum, the following for each task:

- All standards followed in support of these requirements
- A matrix of all deliverables and planned delivery dates
- Task methodologies
- Standard Operating Procedures (SOP's) for all tasks
- A matrix of all personnel (subcontractors and/or consultants) assigned to the program and total aggregate level of effort for all tasks, including position, office location, building access status, and CISA computer equipment (if any)
- Task dependencies and interrelationships
- Contractor organizational structure
- Process management and controls
- Quality control and processes (include the contractor's QCP)
- Any unique hardware and software utilized by the contractor
- Subcontracting plan, including scope and terms of all active subcontracts (if any)
- POCs
- General operating procedures for:
    - Travel
    - Work hours
    - Leave
    - Deliverables
    - Staff training policies
    - Problem/issue resolution procedures

The contractor shall incorporate the Government comments into a final PMP no later than thirty (30) days after the kick-off meeting. Changes to the final PMP may be made with mutual consent of the contractor and the Government.

3.1.3.1 UPDATE THE PROGRAM MANAGEMENT PLAN (PMP)

The PMP is an evolving document that shall be updated with significant changes as required and at least quarterly at a minimum **(Deliverable 8).** The contractor shall work from the latest Government approved version of the PMP.

3.1.4 SUBTASK 1.4 – PERFORM AND MAINTAIN PROGRAM QUALITY CONTROL (QC)

The contractor shall ensure that a high quality of service is maintained throughout the life of this TO. The contractor shall employ realistic and substantial methods and monitoring techniques for improving the overall quality of the CB Mission Support Services. The contractor shall update the QCP periodically to include the following:

- The contractor's overall approach and procedures for communicating with the Government, resolving deficiencies, and identifying potential improvements;
- A description of the contractor's internal review process to include who will perform the review, the frequency, the method and a listing of services/products/capabilities under review;
- The benchmark metrics and measures that will be used to evaluate internal program performance and identify improvement areas and the process for achieving the performance objectives;
- The contractor's approach and procedures for handling corrective action, without dependence upon Government direction, and for implementing potential improvements to program services/products/capabilities.

3.1.4.1 UPDATE QUALITY CONTROL PLAN (QCP)

The contractor shall update the QCP submitted at the Kick-Off Meeting **(Deliverable 9)** periodically as changes in program processes are identified, or annually if no changes are identified.

3.1.5 SUBTASK 1.5 – CONDUCT TRANSITION

A transition shall ensure minimum disruption to vital Government business. The contractor shall ensure that there will be no service degradation during and after transition. The contractor shall propose and implement a Transition-In and Out Plan for the migration of current operations.

3.1.5.1 PERFORM TRANSITION IN

The contractor shall execute their transition in approach to ensure minimum disruption to vital Government business. The contractor shall ensure that there will be no service degradation during and after transition. The contractor shall implement their Transition in Plan (**Deliverable 10**) to facilitate the accomplishment of a seamless transition from the incumbent to an incoming contractor/Government personnel at the award of the TO. The plan shall identify and discuss the existing roles and responsibilities of the incumbent contractor and information expected from the incumbent. The plan shall also identify the roles and responsibilities of the contractor, transition of the CDM PMO support including proposed schedule(s), milestones, and deliverables. The contractor shall identify any actions contemplated on the part of the Government. The Transition-In Plan shall be provided at the Kick-Off Meeting.

3.1.5.2 PERFORM TRANSITION OUT

The contractor shall implement the Transition Out Plan that has been provided NLT ninety (90) days prior to expiration of the TO **(Deliverable 11).** The Transition-Out plan shall facilitate the

accomplishment of a seamless transition from the incumbent to an incoming contractor/Government personnel at the expiration of the TO. The contractor shall identify how it will coordinate with the incoming and or Government personnel to transfer knowledge regarding the following:

- Project management processes
- Points of contact (POC)
- Location of technical and project management documentation
- Status of ongoing technical initiatives and training events
- Appropriate contractor to contractor coordination to ensure a seamless transition.
- Transition of key personnel
- Identify schedules and milestones
- Identify actions contemplated on the part of the Government.

Establish and maintain effective communication with the incoming contractor/Government personnel for the period of the transition via weekly status meetings.

3.1.6 SUBTASK 1.6 – PROVIDE FINANCIAL REPORTING

The contractor shall provide a Financial Report of cumulative expenditures monthly (**Deliverable 12**) via the template provided **(Attachment B – Financial Report Template)** to the COR. The Financial Report shall include, at a minimum, the following:

- Project monthly expenditures and labor hours by CLIN and TO level starting with the current month through the end of the POP.
- Funded levels by CLIN
- CLIN incremental funding and expenditures by government budgetary lines of accounting
- Labor hours incurred to date by CLIN
- Diagram reflecting funding and burn rate by month
- Cumulative invoiced amounts for each CLIN up to the previous month.
- Actual current and cumulative dollars expensed for small businesses compared to TO subcontracting goals.
- Invoice back-up and supporting documentation.

The financial report shall include a break-out and tracking of expenditures of various sources of funding and/or by task/subtask identified by the Government. The Government may request updates to the format based on CISA requirements.

3.1.7 SUBTASK 1.7 – PROVIDE ACCOUNTING FOR CONTRACTOR SUPPORT

CB operates and maintains a secure data collection where the contactor shall report ALL contract manpower (including any subcontractor or teaming partners) required for performance of this TO. In support of streamlined onboarding and personnel accountability, contractors shall completely and accurately populate all required information in the attached **(Attachment C – CWMS Contractor Staffing List Template)**, ensuring accordance with the outlined instructions and formatting guidelines. Throughout the PoP, contractors are required to provide

staffing updates utilizing the forms provided in the attached **(Attachment D – CWMS New Contractor Staffing Form, Attachment E – CWMS Contractor Exit Form, and Attachment F – CWMS Contractor Update Form)**. All updated forms must be documented and submitted to the contractor security mailbox (csd_cb.contractorsecurity@cisa.dhs.gov) within **one week** of the staffing action occurring. If errors are identified, the provided documentation will be returned for remediation by the contractor. Baseline staffing plans are to be submitted in alignment with the prescribed deliverable timeline located in contract award documentation. Post baseline, all contractor personnel supporting this effort shall be accounted for in the Manpower Database prior to begin work on this TO.

3.1.8 SUBTASK 1.4 – CONDUCT QUARTERLY IN-PROGRESS REVIEW (IPR) MEETINGS

The contractor shall conduct a formal In-Progress Review (IPR) Briefing **(Deliverable 13)** at a location approved by the Government or virtually through Microsoft Teams. The IPR shall provide a forum for Government review of progress, planning, and issues related to TO performance. The contractor shall utilize the PMP in its discussion of TO performance. The quarterly IPR briefing shall replace the Monthly Status Briefing Meeting for that month. IPRs shall, at a minimum, include:

a. The status of activities during the reported period, by task area,
b. Project Schedule
c. Previous month and quarter activities by task
d. Planned activities for next month and quarter by task
e. Financial status, and forecast
f. Manpower/security status update
g. Issues
h. Actions required by the Government.

The contractor shall prepare the IPR agenda, Meeting Report **(Deliverable 4)**, and presentation material. IPRs shall be conducted no less than quarterly; however, more frequent IPRs may be required. The IPR is historically attended by an average of seven to 15 total stakeholders, to include contractor personnel, COR, CISA Functional Leads, and other Government resources.

The fourth quarter IPR meeting of each TO year shall act as an overview of the entire TO year and act as a closeout for the ending TO year. The fourth quarter IPR shall include the above IPR requirements, financial reporting information for the year, Master Repository and Procurement Report information for the years, and planned actions required by the contractor and Government.

3.2 TASK 2 – PROVIDE PROJECT MANAGEMENT SUPPORT

Project Management Support is required throughout the organization to assist Government Program Managers in monitoring, tracking and effectively executing their programs.

3.2.1 SUBTASK 2.1 – PROVIDE ENTERPRISE PORTFOLIO MANAGEMENT SUPPORT

Overarching Program Management Office and Enterprise support is required throughout CB to assist the subdivision, branch and section leadership as well as specific program and services management leadership in managing a variety of organizational, project and program activity.

3.2.1.1 SUBTASK 2.1.1 – PROVIDE CDM ENTERPRISE PORTFOLIO MANAGEMENT

The portfolio management section of the CDM PMO is responsible for the project management and oversight activities for all agency activity executed by CDM contracts. Among other traditional project management activities, this includes tracking and monitoring various integrated master schedules (IMS), identifying and assessing project and program risks, and performing general project and agency portfolio tracking and task oversight. The PM section also maintains the CDM program's capability roadmap, which tracks the implementation of CDM technical capabilities at each agency. The government requires direct support to the CDM Portfolio Management Section Chief and Deputy in the execution of the above activities providing an enterprise view of all the activity being executed across the FCEB and status. The contractor shall provide direct support to the PM Section Chief and Deputy in an "action officer" capacity, facilitate the portfolio IPTs, support the DEFEND portfolio teams in engagements with agencies and assist in the overall internal management of the PM section. In addition to the general requirements listed above, the contractor shall support the Government with activities to include, but not be limited to the following:

- Overarching risk management support at the portfolio level. This includes, but is not limited to the following:
    - Working with stakeholders to capture, identify and mitigate risks (**Deliverable 14**) for input into the CDM risk tool (ie, ALMSS or other business intelligence or process tools)
    - Represent the portfolio teams/PM Section Lead at the CDM Risk Review Panels and other working groups.
    - Updating project risks for PMs and Deputy PMs
- Coordinate with DEFEND and Dashboard portfolio teams to update and manage the CDM capabilities roadmap (bi-weekly and/or monthly) (**Deliverable 15**)
- Coordinate with DEFEND and Dashboard portfolio teams to collect and refine DEFEND quad charts (**Deliverable 16**) and other pertinent information for routine PM and/or CDM IPT meetings
- Participate and contribute to the PM section weekly meetings
- Re-organize and maintain the PM Sharepoint collaboration portal
- Coordinate with portfolio managers and deputies to aggregate and consolidate the weekly report inputs. (**Deliverable 17**)
- Support the PM Section Chief and Deputy in developing PM section SOPs, charters, and other process/procedure documentation (**Deliverable 18**)
- Coordinate and manage leadership calendars to support agency and internal engagements

3.2.2 SUBTASK 2.2 – PROVIDE PROJECT LEVEL PORTFOLIO/SERVICE MANAGEMENT SUPPORT

The Government requires specific support at the portfolio and project level. This support focused on the various contracts, initiatives, pilots and portfolios.

3.2.2.1 SUBTASK 2.2.1 – PROVIDE CDM PORTFOLIO MANAGEMENT SUPPORT (PROJECT/CONTRACT LEVEL)

The Portfolio Management (PM) branch of the CDM PMO consists of a Section Lead (PM lead), a Deputy Lead, and PMs aligned to all of the DEFEND orders that each support a portfolio of FCEB agencies, as well as the Dashboard contract.

The DEFEND and Dashboard portfolio teams at the project level are comprised of a PM, Deputy PM, Engineer, Test Representative and COR. Each DEFEND group consists of 5-7 agencies; some of which are comprised of numerous bureaus and components. The number of weekly engagements and contract deliverable/artifact throughput on these contracts is significant. The government requires project management support (per portfolio team, DEFEND A-E and Dashboard) to support the execution of CDM DEFEND/Dashboard contracts. This will require close coordination with various government and contractor representatives to include external agencies and DEFEND Integrators. Occasionally, the contractor shall represent the Government during engagements with agencies. In addition, the contractor shall support the Government with activities to include, but not be limited to the following:

- Support the portfolio teams on regular engagements with agencies in order to track activities, risks, and requirements **(Deliverable 4**)
- Coordinate agency requests for information and inquiries with Portfolio teams and section chief
- Assist in the tracking of capability roll out and milestone completion at participating agencies (**Deliverable 19**)
- Coordinate across PMO sections to ensure DEFEND operational and functional characteristics, requirements or lessons learned are captured and shared (**Deliverable 20**)
- Evaluate and recommend change requests and related documents in coordination with the Government. This also includes participation at technical interchange meetings, design reviews, program management reviews, and other meetings as required.

3.2.2.2 SUBTASK 2.2.2 – PROVIDE QSMO PMO SUPPORT

As the QSMO grows and finds itself operational, the amount of data, documentation, and records increases exponentially. The QSMO PMO requires improved knowledge management and standard, institutionalized quality and performance procedures in place to support its operational verticals. The contractor shall support the Government with activities to include, but not be limited to the following:

- Assist in managing business operations and process improvement activities across the QSMO's various functions (e.g., Services Management, Portfolio Management, Provider Management, Services Innovation Management, Communications Management, Analysis and Evaluation Management, etc.).

- Assist the QSMO PMO functional leadership in establishing working groups and charters, developing procedures and standards for records and deliverable archiving, support the QSMO PMO in performance reporting and management, and serve as focal point for the QSMO's internal process and workflow improvement.
- Develop program metrics that measure success of the program, as well as develop plan to monitor and manage metrics.
- Support the QSMO PMO in providing a consistent level of quality across the QSMO (documentation, consistently demonstrate the value and benefits of QSMO services to agencies and key stakeholder partners and create a customer centric culture for the QSMO).
- Establish criterion to determine what level of review and approval is required for documents published through the QSMO and establish a repeatable and transferable process that will include specific review and control gates by appropriate levels of leadership.
- Gather requirements from across the QSMO and develop an electronic document library as part of knowledge management.
- Support the QSMO PMO in establishing the associated processes required to maintain document integrity, manage access and track the development and submission of documents published by the Program.

3.2.2.3 SUBTASK 2.2.3 – PROVIDE QSMO SERVICES MANAGEMENT (SM) SUPPORT

The Service Management (SM) section within the Cyber QSMO oversees the delivery, and operation of holistic services that strengthen federal agencies' cybersecurity posture. IT Service Management, Readiness Support, and Analysis of Support are the tenets that drive and enable Service Management to play a coordinating, advocacy, and advisory role in improving service-related practices and procedures for customer agencies. The SM section consists of a Section Chief, a SM Team Lead aligned to each of the current service offerings, Vulnerability Disclosure Platform (VDP) and protective Domain Name Service (pDNS) with plans to develop additional service offerings (Mobile, Security Operations Center (SOC), etc.).

There are currently two (2) Government Service Managers aligned to the organization with a plan to scale consistently with the growth and addition of new services (up to 5 Service Managers). The government requires direct support to the SM Section Chief in an "action officer" capacity, support to the Services Management Teams in the facilitation of the portfolio IPTs, engagements with agencies and assist in the overall internal management of the SM section. The contractor shall support the Government with activities to include, but not be limited to the following:

- Assist in the development and execution of QSMO service offerings.
- Participate in and contribute to the tasks required to stand up new Sections with QSMO
- Develop standardized processes for the operation and sustainment of the Service Management Section (**Deliverable 18**)
- Research, define, and implement best practices for Information Technology Service Management (ITSM) support

- Support all services in navigating and coordinating Authorization to Operate (ATO) with various external and internal parties
- Coordinate adequate levels of support to CISA ISSOs to properly protect CISA systems.
- Ensure acquired provider exceeds security requirements.
- Support requirements definition to the solution.
- Draft project plans and provide project management support to assist customers onboard, implement and transition to the new solution (**Deliverable 21**)
- Coordinate with providers on operational related issues

3.2.2.4 SUBTASK 2.2.4 – PROVIDE QSMO PORTFOLIO MANAGEMENT PROJECT MANAGEMENT

The Portfolio Management Section of the QSMO Branch prioritizes and designs the portfolio of shared cybersecurity services for the Cyber QSMO. This section performs the following functions: Customer Analysis and Market Research, Service Prioritization, Initial Service Delivery Model Design, Analysis of Alternatives, Service Catalog Management and Continual Service Improvement. The Portfolio Management section consists of a Section Chief and grow to include governance and service design leads. The contractor shall provide project management support to include, but not limited to the following:

- Assist in the identification and analysis of customer needs and requirements, including CISA/CSD/CB strategic priorities and new directives/guidance.
- Support research on services and capabilities in the federal and commercial marketplaces to meet emerging needs and requirements
- Assist in prioritization of new services/capabilities to create a ranking for inclusion into the Marketplace or enhancement of existent services.
- Support the development of delivery options for selected services or capability bundles within each service, as well as high-level deployment and operating models. (**Deliverable 22**)
- Assist in the analysis of alternatives and the development and facilitation of decision-making for a preferred course of action for a new QSMO service. (**Deliverable 23)**
- Support the maintenance and management of a QSMO Service Catalog including QSMO service taxonomy.
- Develop products in support of continual service improvement.

3.2.2.5 SUBTASK 2.2.5 – PROVIDE QSMO PROVIDER MANAGEMENT PROJECT MANAGEMENT

The Provider Management Section of the QSMO manages relationships with service providers/vendors and their onboarding to the Cyber QSMO Marketplace, including CISA services and Federal Shared Services Providers (FSSP). The contractor shall provide project management support to include, but not limited to the following activities:

- Support creation of memorandum of agreement (MoA) for activities between QSMO.
- Coordinate validation sessions with FSSP, to identify validation activities.

- Support notification of validated offering of FSSP services to Comms/CX for proper identification in the Marketplace.
- Track cost avoidance to the Federal enterprise by the utilization of a FSSP service/s.
- Track quality of service/s provided to end users by FSSPs.
- Assist in the administration of quarterly meetings with FSSPs to provide insight of processes and new service offerings.
- Assist in the development of responses to service inquiries from the Federal enterprise and other internal CISA entities.
- Create, update, and track FSSP Standard Operating Procedures. (**Deliverable 18**)
- Interact with other QSMO Section to ensure proper procedures are followed.
- Provide push and pull documentation activities between the Office of Management and Budget (OMB) Max Portal and QSMO FSSPs Section.
- Assist with the development of quarterly FSSP Meeting activities.
- Provide agenda, send meeting invites, track participation, track meeting action items, provide follow-up minutes. (**Deliverable 4**)
- Assist with the updating of the quarterly reporting template where applicable.
- Track MoA documentation as applicable. (Deliverable 38)

3.2.2.6 SUBTASK 2.2.6 – PROVIDE QSMO SERVICES INNOVATION PROJECT MANAGEMENT

The Services Innovation (SI) section researches, develops, and pilots potential new cybersecurity shared services offerings, partnering with DHS Science &Technology (S&T) and other external stakeholders. The SI section consists of a Section Chief and a SI Team Lead with plans to add additional support as the workload increases and/or as new initiatives or pilots are identified for CB to plan and execute. The contractor shall provide project management support to include, but not be limited to the following:

- Assist in the planning, facilitation and execution of technical exchange or IPT meetings in conjunction with Services innovation initiatives (i.e., examples include ongoing and upcoming pilots such as mobile initiatives, Secure Cloud, O365, Google Workspace, etc.)
- Coordinate and assist with providing regular updates to QSMO leadership and other sections to provide awareness of SI activities.
- Assist in updating standard reports
- Provide product and deliverable artifact management support
- Provide qualitative and quantitative analysis and research in support of new and future initiatives
- Support data analysis and operations research.

3.2.2.7 SUBTASK 2.2.7 – PROVIDE QSMO CX AND COMMUNICATIONS PROJECT MANAGEMENT

The Cyber QSMO CX and Communications Section manages the internal and external communications regarding service offerings and ongoing activities within the QSMO. This section oversees and manages the design and administration of the Cyber QSMO Marketplace, ensuring shared services are accurately categorized and featured in accordance with QSMO

designation, CISA, NIST, and other regulatory standards. The CX and Communications Section consists of a Section Chief with plans to add additional support as the workload increases. The contractor shall assist the Government in providing QSMO CX and communications project management support to include, but not limited to the following activities:

- Develop and update standards for the Marketplace.
- Support the service acquisition lifecycle for customers from service validation to adoption and evaluation support.
- Coordinate with IPT members in the development and sustainment of the Marketplace platform, content and offerings.
- Coordinate Marketplace customer engagement with internal and external entities.
- Management of the internal documentation supporting the Marketplace.

3.2.2.8 SUBTASK 2.2.8 – PROVIDE ANALYSIS AND EVALUATION PROJECT MANAGEMENT

The QSMO's Analysis and Evaluation Office (A&E) analyzes and evaluates service-related data, metrics, and trends to improve and enhance the Cyber QSMO's service offerings to ensure services meet customers' needs. continuously evaluate both the environment within which QSMO services are being deployed, as well as the impact of QSMO services. With proper support, the QSMO will be better equipped to make tactical and strategic decisions to continuously improve how it serves its customers and users. The QSMO requires a variety of data and analytic insights to drive decisions around the QSMO portfolio. The contractor shall provide support to QSMO A&E project management and PM support to include, but not limited to the following:

- Identify relevant data sources.
- Establish processes and systems to collect, extract, transform, load, and analyze relevant data into analytical models and frameworks. (**Deliverable 18**)
- Design and execute models and frameworks.

The contractor shall assist the Government in providing a broad understanding of the current market for cybersecurity services and products. The contractor shall support market research on vendors, capabilities, customers, risks, and potential fit with FCEB requirements (and potentially SLTT requirements) The QSMO requires support in the development and testing of frameworks and methodologies that assist the QSMO in determining baseline and optimal cybersecurity service requirements for the FCEB, evaluating alternative service delivery models, and creation of business cases to support decision-making. (**Deliverable 24**). The contractor shall assist the Government in the development and testing of frameworks and methodologies that assist the QSMO in determining baseline and optimal cybersecurity service requirements for the FCEB, evaluating alternative service delivery models, and creation of business cases to support decision-making. The contractor shall support QSMO A&E with developing strategies to measure the impact and effectiveness of CISA cybersecurity services (**Deliverable 25**). The contractor shall assist with analysis efforts into CISA cybersecurity services to identify challenges, opportunities, and areas for improvement. This analysis may result in the

establishment of service specific strategies, awareness documentation, or improvement plans (**Deliverable 26**).

3.2.2.9 SUBTASK 2.2.9 – PROVIDE CYBER THREAT INTELLIGENCE SHARING (CTIS) PROJECT MANAGEMENT SUPPORT

The CTIS branch has matured their information sharing initiatives and platforms into an enabling capability, enhancing the .gov networks. Despite their continued success, the CTIS branch plans to evolve these offerings into enterprise capabilities. The CTIS branch requires planning and project management support to mature the threat intelligence sharing programs and assist in agency and CISA-internal engagements. The contractor shall provide the following support to include, but are not limited to:

- Assist in managing CTIS branch business operations and process improvement activities
- Coordinate agency engagements, working groups and IPTs and technical information exchange meetings Support includes several interagency, private sector and SLTT ongoing working groups which CTIS leads on behalf of CISA
- Provide agenda, send meeting invites, track participation, record meeting minutes, track meeting action items and taskers, provide follow-up meeting minutes and assist with meeting logistics.(**Deliverable 4**)
- Assist the CTIS leadership and Threat Intelligence in coordination, managing contract deliverables, developing procedures, standards for records, documentation and products.
- Assist in the development of responses to contract and service inquiries from the Federal enterprise and other internal CISA entities.

3.2.3 SUBTASK 2.3 – PROVIDE SUPPORT TO STRATEGIC INITIATIVES AND WORKING GROUPS

Recent cyber-attack campaigns have underscored the critical need to assist agencies in identifying the most significant cybersecurity risks and driving timely remediation of security weaknesses and overall improvement in cyber risk capabilities and posture across the federal enterprise. Remediation efforts on the heels these incidents have also highlighted gaps in the way that CSD and CB assists agencies, with a need to better bridge operational and programmatic support activities executed by each of the Subdivisions to achieve continuity and build upon progress. The contractor shall provide project management and planning support to strategic initiatives and work groups associated with delivering capability to the federal enterprise. The contractor shall assist with developing and designing strategic plans in accordance with changes in the operating landscape, priorities and initiatives of the organization (**Deliverable 25**). In addition, the contractor shall evaluate and provide recommendations and administrative support for the strategic plan's goals, objectives, and corresponding performance measures. This may require analysis and facilitation of focus groups to ensure that the plan remains on-track and to assess whether other strategic opportunities or organization objectives are needed. These plans should be agency centric and consider the challenges oriented around delivering implementation plans across the.gov enterprise. Additionally, the contractor shall assist in the implementation

and execution of the strategic plan and other initiatives as identified. The contractor shall assist in the development of future strategic plans and associated program unit plans.

The contractor shall assist in developing operational plans and roadmaps to support the program strategies and implementations of capabilities (**Deliverable 15**). The operating plans shall support accountability for initiatives and include measurable performance metrics. As required, the contractor shall implement performance improvement projects, evaluate programs, and identify barriers and opportunities to achieve strategic objectives.

3.2.4 SUBTASK 2.4 – PROVIDE CRITICAL ASSETS AND ENTERPRISE IMPLEMENTATION PROJECT MANAGEMENT SUPPORT

The EI Branch requires project management support to assist in the ongoing targeted assessments of agency systems and risk profiles. EI coordinates and facilitate risk reduction activities across the FCEB through the High-Value Asset (HVA), FISMA, Cyberstat and Standards support programs. The contractor shall provide project management support to include, but is not limited to:

- Develop and maintain artifacts which provide communication to all internal and external stakeholders
- Maintain agency risk registry, reports and risk categorization reports for the various systems (**Deliverable 14**)
- Assist the government in the Analytic Hierarchy Process (AHP)-based pairwise comparison process with CISA, OMB, NIST, and Federal agencies resulting in the development of the revised Federal High Value Asset Enterprise Prioritization (FHE) Paper Version 2.0.
- Develop the process to align Tier 1 and Non-Tier 1 categorization with the revised HVA Strategy (new HVA assessment and CE evaluation approach).
- Assist in the development of the HVA modernization template and corresponding Cyberstat workshops.
- Assist the government in providing oversight and compliance with planning, policy, and guidance actions and provides direct assistance to improve agency accountability
- Plan and coordinate agency engagements. The contractor shall support regular engagements with agencies in order to track general activities, risks, and requirements
- Identify and track agency challenges and validates FCEB priorities through trends analysis and interagency relationship management.
- Analyze and research issues and priorities to assist in developing FCEB-wide strategic planning and frameworks, programming approaches, policy guidance, and recommendations.
- Support FISMA and Cyberstat Programs.
    - Convene and participate in FISMA discussions
    - Establish FISMA frameworks
    - Establish, facilitate and support Cyberstat Workshops. The contractor shall provide the following support to include, but not limited to the following:
        - Draft and update an annual CyberStat Program CONOPS.

- Draft an escalation plan for agencies that are not making progress in resolving their security challenges
- Draft and update SOPs for conducting a CyberStat workshop, leading a Technical Assistance Engagement, reviewing the CyberStat mailbox, and maintaining the OMB MAX CyberStat site.
- Ensure quality assurance processes are in place and used for the following tasks to include, but not limited to the following:
    - Research and analysis of GAO, IG and FISMA reports.
    - Prioritization of workshop topics and participating agencies
    - Recommend, improve and advance planning for workshops.
    - Analyze agency best practices and lessons learned.
    - Identify Subject Matter Experts (SMEs) and coordinate workshop content
    - Develop policy and strategy templates.
    - Develop briefing slides and talking points.
    - Provide workshop logistics.
    - Prepare emails to agency executives.
    - Maintain records keeping.
    - Escalation to a Technical Engagement and Assistance (TEA) engagement.
    - Coordination and preparation of materials and logistics for the TEA.
    - Conducting a TEA and documenting outcomes.
    - Utilizing automated or manual reporting to validate continued progress in resolving security challenge.
    - Summarizing the TEA engagement in a closeout report.
    - Uploading content to the CyberStat page on the MAX website
    - Preparing agenda and documenting actions resulting from bi-weekly CyberStat meetings with OMB

- Support annual FISMA reporting
    - Review and edit of agency FISMA narratives
    - Support performance summary incident reconciliation
- The HVA PMO within the EI Branch must continue a comprehensive engagement with agencies to ensure system profiles are prioritized and risks are tracked and reported. The contractor shall coordinate agency requests for information and inquiries with HVA program leadership and maintain agency HVA system profiles (**Deliverable 27**)
- Advise and assist the Cybersecurity Standards Area Lead during the development and revision of government-wide cybersecurity policies and assessing compliance of service providers, including ensuring business needs/requirements are defined and met
    - Assist in managing and identifying the approaches and development of standards needed to successfully implement the identified recommendations, approaches, and guidance across the FCEB.

3.2.5 SUBTASK 2.5 – PROVIDE TRUSTED INTERNET CONNECTIONS (TIC) PROJECT MANAGEMENT SUPPORT

The TIC program began with an objective of creating the first federal perimeter security baseline. Specifically, OMB tasked DHS with modernizing the TIC initiative to accelerate the adoption of cloud, mobile and other emerging technologies. CISA has refined specific guidance in support of D/As in order to identify reference architectures for TIC use cases. To ensure continued TIC program success, the TIC PMO requires project management support services. The contractor shall provide project management support to include, but not limited to the following:

- Develop and share TIC guidance in order to keeps pace with evolving technology, agency needs, vendor engagement, and remains aligned with CISA's Cloud Strategy.
- Direct support during individual agency/interagency and industry engagements
- Assist in the coordination and execution of IPT and working group activities
    - Technical discussions and multi-agency working groups comprised of representatives from the Chief Financial Officer (CFO) act agencies and assist with the adjudication of agencies' technical recommendations.
- Participate in agency technical information exchange meetings as part of ongoing pilots and initiatives
- Assist with expanding the program to be able to support long-term pilot management and use case lifecycle tasks, and agency education and conformance management.

3.2.6 SUBTASK 2.6 – PROVIDE CUSTOMER EXPERIENCE (CX) PROJECT MANAGEMENT SUPPORT

The Contractor shall provide customer experience project management to assist the Government in understanding customer experiences and needs to help CISA develop and provide the tools, services and guidance needed by agencies to protect their environments. Customer experience project management support includes, but not limited to the following:

- Coordinate and manage customer engagement the activities and tasks across all teams and collect feedback.
- Assist in efforts to standardize the solicitation of feedback from customers to create consistent feedback approaches.
- Support the improvement of the feedback collection process to ensure it transitions into actionable data.
- Assist in facilitating agency focus groups and engagements (to include but not limited to Quarterly Federal Cybersecurity Advisory Council Meetings, Advisory Forums, and CX special events). Support includes Provide agenda, develop meeting content, talking points, send meeting invites, track participation, track meeting action items, provide follow-up minutes, executive summaries (**Deliverable 4**).
- Perform targeted research and support external customer engagements to assist in recommending design and redesign of services and products across CS and CSD
- Identify and educate internal stakeholders on industry best practices and approaches to enhance their own programs and services. Provide support to assist in the adoption and

implementation of a human-centered design approach to engaging customers in the service development process.

- Support change management, business process engineering, transition management, implementation of major performance improvement initiatives/programs, communications associated with major initiatives, risk assessment, and organizational transformation and culture change.
- Conduct qualitative, quantitative, and historical research to mine customer insights and understanding.

3.2.7 SUBTASK 2.7 – PROVIDE FEDERAL ENTERPRISE IMPROVEMENT TEAM (FEIT) SUPPORT

Recent cyber-attack campaigns have underscored the critical need to assist agencies in identifying the most significant cybersecurity risks and driving timely remediation of security weaknesses and overall improvement in cyber risk management across the federal enterprise. FEIT is charged with defining federal enterprise-level strategic efforts and supporting agencies in developing and implementing tailored cybersecurity improvement plans. This team brings together and extends capabilities and functions from across CSD to assist with analyzing, prioritizing, and mitigating the most pressing cybersecurity risks for the benefit of all civilian agencies. Through dedicated agency portfolio teams and targeted technical and programmatic consultation, the FEIT will work directly with agencies and drive proactive improvement based on CISA analysis.

The FEIT Team is composed of agency portfolio management support including federal Security Operations Center (SOC) support and product development that requires targeted project management, administration, and planning to support external engagements with Departments and Agencies (D/As) and internal cross-functional communications and updates.

3.2.7.1 SUBTASK 2.7.1 – PROVIDE AGENCY PORTFOLIO MANAGEMENT AND SUPPORT

The Agency Portfolio Management & Support directly supports FEIT engagement efforts at the executive level and with agency security operations centers. The contractor shall support dedicated agency teams to enable a deeper understanding of each agency's existing capabilities, challenges, risks, and their overall risk picture. The contractor shall assist the Government in developing and executing operational plans in response to FCEB cybersecurity incidents or threat activity, supporting remediation and mitigation efforts in response to directives, and driving agency engagement, messaging, technical exchanges to improve agency cyber defense operations. The contractor shall assist the Government in providing the following agency portfolio management and support to include, but not limited to the following:

- Planning and organizational standup of the FEIT and provide support to full operating capacity.
- Provide program management support for Cyber Risk Officers and Fed SOC liaisons with agency engagements. Support includes providing dedicated CISA engagement to agencies both at the executive CISO/CIO level and to Agency SOCs. The contractor shall provide subject matter expertise providing a deep agency-level understanding and strong working relationships at the executive and SOC level.

- Maintain a comprehensive picture of CISA/CSD support to agencies across functions.
- Track, monitor and facilitate FEIT programmatic engagements and CISA support to agency operational activities, track agency requests, risks requirements, and progress against priority efforts identified through agency improvement planning.
    - Maintain a comprehensive picture and up to date tracking of FEIT and CSD engagement with agencies at enterprise and agency levels.
    - Perform logistical and administrative support for direct engagements and meetings (documentation, notes, meeting planning/facilitation).
    - Develop SOPs for logistical and administrative support for direct engagements and meetings **(Deliverable 18).**
    - Conduct cross-functional workshops, design workshops, and other facilitated interactive sessions
    - Develop customer engagement strategies and models
- Perform research that better understand stakeholder needs to inform improvements to products, services, policies, and processes. The contractor shall conduct customer and stakeholder interviews, interview guides, notes, and analysis. The contractor shall perform agency, customer, and stakeholder analysis, conduct surveys and resulting analysis, research plans, reports, and associated artifact. The contractor shall creatively gather and package compelling customer feedback, research, and other data to develop insights to support leadership decision-making.
- Plan, manage, and execute on an idea from concept to launch to meet key milestones and real customer needs
- Provide perspective on quantitative and qualitative data to help stakeholders understand their users; identify and quantify problems; and embark on new research areas worth exploring through innovative methods.
- Review, evaluate, distill and synthesize data to uncover issues, identify trends and provide insights that drive organizational strategy
- Strategic communication support with agencies to include assisting the Government in developing and updating a FEIT Strategic Communication Plan **(Deliverable 28).** Assist with coordinating integrated agency support activities and communicate agency priorities through tailored agency improvement plans
- Provide training and specific FEIT on-boarding materials for new employees.
- Track and coordinate agency requests for information, inquiries and priority needs.
- Coordinate, participate, and attend meetings as required.
- Draft meeting reports to document results of meetings and action items **(Deliverable 4).**

3.2.7.2 SUBTASK 2.7.2 – PROVIDE PRODUCT DEVELOPMENT SUPPORT

Product Development is focused on providing agencies with a clear understanding of the most pressing cybersecurity risks and a prioritized set of actions to help guide them toward mitigating those risks. The contractor shall assist the Government in setting forth the comprehensive risk picture and Agency Cyber Improvement Plans to guide the FEIT's priority efforts communicated by the Agency Portfolio Teams. Product Development has two core components: Insights, providing the critical data and input necessary to set improvement priorities and understand both

collective FCEB risk and specific risks and challenges for an agency; and Deliverables, focused on the development of FEIT products that will form the foundation of the FEIT engagement and priority efforts with agencies. The contractor shall assist the Government in providing the following products to include, but not limited to the following:

- Develop documentation, SOPs, RACI's and approaches for leveraging CSD insights, conducting analysis, and developing a product line.
- Provide advisory and consultation support to assist agency implementation of improvement plans.
- Develop FEIT products such as tailored Agency Cybersecurity Improvement Plans, related implementation guidance, and any other enabling work products (e.g., templates, sample policies and processes, recommended configurations) **(Deliverable 26).**
- Develop and update timelines and monitor and track FEIT deliverable activities.
- Maintain a progress tracker measuring goals and objectives identified in agency cyber improvement plans.

3.2.8 SUBTASK 2.8 – PROVIDE PROJECT MANAGEMENT SUPPORT (OPTIONAL)

As the cybersecurity landscape continues to evolve and mature at a rapid pace the Government envisions that over the TO PoP the need to surge, expand capacity and capabilities, realign and adjust priorities, and increase contractor support in order to meet emerging threats, support technology transformation and support enterprise cybersecurity services management in support of its national stakeholders and maintaining its role as the nation's lead for federal cybersecurity risk governance. Additionally, over time CISA intends to expand relationships to include support additional levels and cybersecurity program units within each agency as well as State, Local, Tribal and Territorials (SLTTs) entities.

CB requires increased project management to support consistent with all of the Task 2 activities identified above to maintain cybersecurity readiness, bolster enterprise capabilities and protections, and increases the community's capacity to adequately manage cyber risk in support of its stakeholders.

Additionally, as Capacity Building matures and assumes additional roles and responsibilities for federal security, the organization may require support in establishing and maintaining one or more program management offices. This would drive additional requirements for direct project management, quality control and performance management, risk management and robust knowledge and data management support.

For example, the DOTGOV Act recently transitioned the DOTGOV program from GSA to CISA in April 2021. As such CISA will begin to manage the program and begin operational administration. The .gov top-level domain (TLD) is critical to the availability and integrity of thousands of online services relied on by federal, state, and local governments throughout the United States – and their millions of users. As it underpins communication with and within these institutions, all aspects of .gov's administration have cybersecurity significance and should be carefully managed.

The .gov TLD is part of the global domain name system (or DNS), a distributed technology that is central to the internet's utility and usability. Because everything it touches is tech-centric, the

management of the DotGov Program requires project management support to assist the Government in conducting quality oversight and execution of the program. The contractor shall assist the Government in providing project management to include, but not limited to the following:

- Interface with agencies, respond to inquiries and questions and track and follow-up on requests.
- Administrative support of reviewing .gov domain names to include managing and track domain names and renewal dates
- Maintain and update web-site content.

3.3 TASK 3 – PROVIDE PROGRAM ACQUISITION SUPPORT

Within CB, CDM is an ACAT I program with extensive reporting and oversight requirements. The CDM PMO is required to engage with and provide regular updates to external and DHS internal stakeholders. The government requires assistance in developing products and managing the various program acquisition artifacts and information. Additionally, as CB matures over the PoP other programs may evolve and be considered to become programs of record within the Department. As such, the contractor shall provide support to the Government in strategizing the validity of evolve to acquisition program status and if programs with CB become acquisition programs of record the contractor shall be required to support as described within this Task.

3.3.1 SUBTASK 3.1 – PROVIDE PROGRAM ACQUISITION SUPPORT

The Program Lifecycle Support (PLS) Branch is responsible for the maintenance of the programmatic plans and strategy for the lifecycle of the CDM program. Specifically, they are charged with developing and maintaining the Acquisition documentation and artifacts that convey program health and status. The PLS section requires assistance in managing the various program planning and acquisition requirements. The contractor shall support the government with acquisition activities to include, but not limited to the following:

- Develop programmatic documentation to include:
  - Acquisition Review Board (ARB) briefing, any briefing leading up to the ARB and associated reference materials. (**Deliverable 2**)
  - GAO or external RFI responses
  - Operational Requirements or program strategy documentation (**Deliverable 29**)
  - Affordability and/or Cost RFIs
  - Acquisition Performance and Planning Guidance

3.3.2 SUBTASK 3.2 – PROVIDE PROGRAM LIFECYCLE LOGISTICS SUPPORT

The CDM Program requires a Lifecycle Logistics support to logistics reporting requirements of the program. This contractor shall coordinate across the program to capture affordability and cost drivers, interact with external and supported organizations to ensure lifecycle requirements are met, and manage information flow regarding the needs of agencies from a logistics perspective. The contractor shall support any activities associated with CDM supply chain management requirements.

3.3.3 SUBTASK 3.3 – PROVIDE QUALITY AND RECORDS MANAGEMENT

As the CDM PMO grows, the amount of data, documentation and records increases, exponentially. The need for knowledge management and institutionalized quality procedures has also grown. The government requires support to effectively manage business operations and process improvement activities across the Sections of the CDM PMO (ie, Engineering, PM, Architecture and Integration, PMO support and Test). The contractor shall assist the CDM Leadership Team in establishing working groups and charters, developing procedures and standards for records and deliverable archiving, support the CDM PMO in database and share drive management and serve as focal point for process and workflow improvement.

3.3.4 SUBTASK 3.4 - FUTURE PROGRAM ACQUISITION SUPPORT (OPTIONAL)

As CB matures over the PoP other programs may evolve and be considered to become programs of record within the Department. As such, the contractor shall provide support to the Government in strategizing the validity of evolve to acquisition program status and if programs with CB become acquisition programs of record the contractor shall be required to support as described within this Task.

The contractor shall support the Government with activities to include, but not be limited to the following:

- Develop and manage strategic management lifecycle documentation (e.g., Annual Operating Plan, SOPs, etc.); maintain existing and develop new required program of record materials (e.g., Acquisition Strategy); maintain existing and develop new required investment/acquisition program materials; develop new internal and/or external program-related RFI responses; and plan and develop senior level presentations and briefings.
- Support coordination across the program's operational verticals and cross-cutting support horizontals to: 1) capture affordability and cost drivers, 2) ensure lifecycle requirements are met, and 3) manage information flow regarding the needs of customers and users.
- Develop, implement, and maintain tools/databases or reporting systems required by the PMO that may be necessary for Program and or project management and tracking.
- Develop and maintain the Integrated Master Schedule (IMS), which will cross all ~~QSMO~~ program functional areas, both operational and supporting. In addition, the contractor shall support the Government with activities to include, but not be limited to the following:
    - Review all schedule inputs to inform the overarching Program IMS;
    - Provide schedule development support at the functional level;
    - Track Program milestones to support external guidelines and reporting timelines;
    - Provide schedule analysis to integrate functional project level milestones into Program;
    - Support risk and priority management on functional and Program level milestones and projects.
- Expand and/or surge support to 3.3.1 Subtask 3.1 – Provide Program Acquisition Support, 3.3.2 Subtask 3.2 – Provide Program Lifecycle Logistics Support, and 3.3.3

Subtask 3.3 – Provide Quality and Records Management as CB mission and priorities expand and evolve.

3.4 TASK 4 – PROVIDE PRODUCT MANAGEMENT SUPPORT

The Acquisition and Budget Branch procures, tracks and maintains the footprint of all tools procured within the organization. Majority of the tools procured are in support of the CDM Program; however, over the PoP, and as the CB programs evolve, additional tracking and oversight may be required.

3.4.1 SUBTASK 4.1 – PERFORM APPROVED PRODUCTS LIST ADMINISTRATION AND MANAGEMENT

The Acquisition and Budget Branch maintains a list of approved products that supports the various CDM solutions. The CDM PMO charters a technical evaluation team which reviews vendor submissions of products for inclusion on the APL. The contractor shall support the monthly evaluation of new and updated product submissions for consideration to be added to the APL. The contractor shall provide the following support to include, but not limited to the following:

- Facilitate and manage the intake of all APL submissions.
- Conduct conformance checks to assure that the product submission are in accordance with APL standards.
- Update, track and manage submissions to ensure high fidelity data
- Assemble and file submission documents on SharePoint and Maestro/Jira and communicate with the technical review team when files are ready for Tier 2 review. Upon Tier 2 completion, the contractor shall prepare the package for Tier 3, or CISA Final Technical Review
- Conduct APL closeout activities, including notifying submitters of their package status, notifying GSA Schedule 70 of product acceptance, and prepare a monthly workbook of what products need to be added, modified, or deleted from the APL(Deliverable).
- Track, report, query, and provide monthly metrics of APL status (**Deliverable 30**)
- Update published APL with new, modified, and deleted products **(Deliverable 31)**
- Manage content on A&B APL webpage, including publishing monthly APL
- Manage, update and administer APL and all associated supporting documents to include VPATs, EULAs and SCRM plans.
- Assemble and file supporting documents on OMB Max.
- Assist the Government in review, update and enhancements of SCRM plan/questionnaire requirements to better assist an Agency or ordering activity in making a better-informed risk decision when considering or using products from the APL.
- Assist the government in developing and recommending improvements to the data management and automated solutions currently in place (**Deliverable 26)**
- Assist in managing APL Quarterly Audit Process (products are reviewed every three years), which includes communicating to vendors removal and re-submission of products
- Assist with updating SOPs for the APL process (**Deliverable 18**)
- Assist in responding to data calls.

3.4.2 SUBTASK 4.2 – PERFORM ORDER PRODUCT REVIEW AND TRACKING

The contractor shall assist the government in performing order product review and tracking to include, but not limited to the following:

- Review Request to Initiate Purchase (RIPs) to ensure conformance with the template. Identify and recommend revisions and approval to CORs.
- File Requests to Initiate Purchases (RIPs) on SharePoint. Maintain an up-to-date inventory of all RIPS. **(Deliverable 32)**
- Confirm GSA listed pricing and CDM SIN utilization on GSAAdvantage!®
- Confirm part numbers, quantities, and pricing aligns with historical data and forecasting for renewals.
- Update Master License Tracker with RIP information and outyear costs.
- Assist with updating SOP for RIP review. (**Deliverable 18**)
- Update and track Pricing Agreement tracker, which outlines all pricing agreements made across the DEFEND Orders.
- Monitor Pricing Agreement tracker for renewal dates to ensure that option year executions are on track.
- Recommend and update RIP template as needed
- Assist the Government in responding to data calls

3.4.3 SUBTASK 4.3 – PERFORM LICENSE MAINTENANCE TRACKING

The contractor shall perform license maintenance and tracking to include, but not limited to the following:

- Update Master License Tracker with new RIPs and after purchase is complete (DD250 signed)
- Update corresponding reports on cost savings, top manufacturers, SIN utilization, etc.
- Review deliverables as they pertain to license procurements and cost savings.
- Prepare and update forecasting reports on Agency product spend on an annual basis (**Deliverable 33**)
- Assist with overseeing the and tracking of agency product procurements and renewals in accordance with OMB Memorandum M-21-02, *Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements* (or any new directives or memorandums). Support includes, but is not limited to the following:
    - Track agency responses and updates the License Maintenance Tracker
    - Assist with updating M-21-02 Acquiring Capability internal and external process documents or any forthcoming memorandums.
    - Ensure the M-21-02 communication plan is executed in accordance with the plan. Support includes drafting correspondence to agencies about licenses, routine monitoring of license renewal date and escalating at-risk licenses to AB and CDM leadership.
- Assist with developing SOPs and process improvement documentation (**Deliverable 18**).

3.4.4 SUBTASK 4.4 – PERFORM VENDOR/OEM/TOOL COORDINATION

The contractor shall preform vendor/OEM tool coordination support to include, but not limited to the following:

- Coordinate weekly vendor capability briefings on behalf of CSD/CB. Coordination includes pre-meeting activities such as preparing the vendor for the briefing, collecting the presentation ahead of time, sending out correspondences and reminders, and overall management of logistics.
- Document any notes, technical assessments on leveraging technology/capabilities briefed or follow-up items identified during vendor briefs (**Deliverable 4**).
- Complete after meeting activities, including, but not limited to, tracking attendance count, updating the Vendor Access database with point of contact information and engagement date, composing and sending out thank you emails to the vendors and attendees, and filing and archiving all meeting documents on Microsoft Teams and SharePoint.
- Manage, compile, and file the vendor surveys- including the survey for interested vendors and the after-action survey.
- Maintain the list of pending vendors and distribute to AB leadership weekly
- Recommend and develop ways to improve vendor engagements.
- Conduct market research on vendor capabilities
- Assist with developing SOPs and other documentation
- Respond to ad-hoc data calls

3.4.5 SUBTASK 4.5 – PERFORM PRODUCT LIFECYCLE PROCESS IMPROVEMENT AND PRODUCT MANAGEMENT SUPPORT (OPTIONAL)

The contractor shall perform, assess and recommend product lifecycle process improvement to include, but not limited to the following:

- Analyze and examine the current product management process to make updates and recommendations that include Federal/DoD and Industry best practices.
- Analyze existing buying methods, review lesson learned and recommend alternatives and new approach to more efficiently and effectively procuring, administrating and managing products.
- Provide continued support for administering subsequent procurement strategies.
- Design and develop an automated solution to manage, track and administer products.
- Expand and/or surge support to Subtask 4.1 – Perform Approved Products List Administration and Management, Subtask 4.2 – Perform Order Product Review and Tracking, and Subtask 4.3 – Perform License Maintenance Tracking as CB mission and priorities expand and evolve.

3.5 TASK 5 – PROVIDE BUDGET AND FINANCIAL MANAGEMENT SUPPORT

The Acquisition and Budget Branch is responsible for leading all CB Budget and Financial Management activities. The contractor shall assist the Government in supporting the Planning, Programming, Budgeting and Execution (PPBE) process, provide subject matter expertise on

general appropriations law, understand and track DHS timelines and budget policy, and experience communicating with program leadership and external entities, such as CISA, DHS, PA&E, OMB and pulling together executive-level communications for Congress and other stakeholders. Specifically, for budget formulation, the contractor shall have an understanding of the DHS acquisition process and milestones, budget process and best practices as well as experience in impact analysis and what-if scenarios. For budget execution, the contractor shall provide subject matter expertise in accounting and general knowledge of FFMS and financial management and reporting and working with large data sets.

3.5.1 SUBTASK 5.1 – PERFORM BUDGET FORMULATION

The contractor shall assist the Government in performing budget formulation support to include, but not limited to the following:

- Support planning with preliminary strategic planning and alignment to CISA's goals and planning guidance.
- Prepare CB's annual budget requests according to the DHS PPBE iterative process, LCCE outputs, DHS/CISA/CSD annual guidance, and CB internal planning.
- Develop justification material during the budgeting phase of the PPBE cycle. The contractor shall collect data and perform impact analysis in support of the government's decision making processes related to the annual DHS Resource Allocation Decision (RAD), Office of Management and Budget (OMB) budget submissions, responses to OMB pass-back levels, and development of expenditure plans.
- Develop the Capital Investment Plan (CIP) and Program Decision Option (PDO) documents based on prioritization of mission requirements.
- Develop impact statements; OMB justification and inputs to the Exhibit 300 based on the RAD; and Congressional Justification/President's Budget Request based on pass-back/draft spend plan.
- Collect data and perform impact analysis in support of the government's decision-making processes related to developing impact statements; OMB justification and inputs to the Exhibit 300 based on the RAD; and Congressional Justification/President's Budget Request based on pass-back/draft spend plan.
- Assist in the formulation and planning of program and project budgets including assisting the government with managing the DHS Future Year Homeland Security Plan (FYHSP).
- Develop detailed multi-year financial plans including estimates, justification of assumptions, research, and analysis.
- Draft and track all budget projections, descriptions, justifications and impact statements and analysis.
- Analyze the information within specific budget documentation to summarize the differences between formulation data and actuals.
- Recommend alignment of budgets with strategic and programmatic goals, and adherence to fiscal guidance and DHS budget policy.
- Review financial documents and plans for impact on program objectives and requirements.

- Draft and prepare financial and budget briefings including spreadsheet and graphic presentations **(Deliverable 2).**
- Subject matter expertise to support the government in statistical and financial analysis as needed.
- Track all budget requests and responses in a Budget/Financial Management Library.

3.5.2 SUBTASK 5.2 – PERFORM BUDGET EXECUTION

The contractor shall assist the Government in performing budget execution support to include, but not limited to the following:

- Fiscal technical expertise and guidance to CBs AB.
- Develop, review and implement project-level budgets, spend plans and Congressional Expenditure plan; and conduct regular and recurring reviews of resource utilization to identify issues that might impact the program's overall objectives.
- Analyze Execution Stage of current Fiscal Year (FY) actions/taxes/re-appropriations/rescissions within the Agency.
- Develop and prepare routine, periodic reports on the allocation, status, tracking, commitment, obligation, and expenditure of funds.
- Assist the government with the government's Budget Change Request process. As new requirements emerge throughout a fiscal year, any changes to the baseline funding levels in the annual spend plan are requested via the government's Budget Change Request process.
- Analyze variances and reporting of status of funds reports. The contractor shall assist the government in developing and updating financial processes and procedures for adequately accounting for and safeguarding the funds allotted for program and projects.
- Support the procurement request process and supporting tracking responsibilities, as well as support reporting to AB/CB Branch Leadership.
- Draft, identify and track unfunded requests (UFRs). Draft justifications and impacts. Recommend trade-offs within CB's budget to support must pays.
- Develop briefs and reports on corresponding budget execution plans.

3.5.3 SUBTASK 5.3 – PROVIDE FINANCIAL MANAGEMENT

CB requires financial oversight and management support for the entire organization. This support will focus on both contract financial management as well as general program financial health and monitoring. The contractor shall support the government with financial services to include, but not limited to the following:

- Provide acquisition data analytical support for contracts/TOs. This support includes but is not limited to: developing financial trend analyses of contracts and task orders to determine the financial health of the contracts/TOs.
- Support the government CORs with contract execution activities such as organizing and tracking contract invoices and deliverables, and monitoring burn rates, analysis of advance liquidations

- Assist the government in the development, review and implementation of project-level budgets and spend plans; and conduct regular and recurring reviews of resource utilization to identify issues that might impact the program's overall objectives.
- Assist the government with the development and preparation of routine, periodic reports on the allocation, status, tracking, commitment, obligation, and expenditure of funds.
- Assist the government in the preparation and processing of funding documents, the analysis variances and reporting of status. The contractor shall assist the government in developing and updating financial processes and procedures for adequately accounting for and safeguarding the funds allotted for program and projects.
- Assist CORs with contract closeout tasks including researching and analysis of UDOs, final invoicing, and IPAC status.
- Develop, implement and maintain tools/databases or reporting systems that may be necessary for program and or project management and tracking.
- Assist with tracking of accountable property within CB to include:
    - Completion of invoice and DD250 reconciliation review and analysis
    - Data entry of all external stakeholder accountable property data by project within designated format to ensure additional information can be provided to each stakeholder on a Quarterly Basis.
- Track all PCARD, Training, and Travel against the annual budget and ensure available funding before making recommendations on approval status.

3.5.4 SUBTASK 3.5.4 – PROVIDE BUDGET AND FINANCIAL MANAGEMENT SUPPORT (OPTIONAL)

The contractor shall expand and/or surge support to 3.5.1 Subtask 5.1 – Perform Budget Formulation, 3.5.2 Subtask 5.2 – Perform Budget Execution, and 3.5.3 Subtask 5.3 – Provide Financial Management as mission and priorities expand and evolve.

3.6 TASK 6 – PROVIDE COMMUNICATIONS AND OUTREACH SUPPORT

The contractor shall assist the government with stakeholder outreach and communications support. This task includes supporting the government in ensuring the flow of accurate and integrated communications to internal as well as external stakeholders like other DHS organizations, FCEB, state and local government, senior leadership, stakeholders, industry, and vendors. Additionally, this task shall provide support to coordinating communications among stakeholders, integrating disparate streams of information across the CB organization; assist with speaking engagements and events; as well as design and develop communication products and collateral. The contractor shall provide communications and outreach support to CB as well as directly to CB Subdivisions.

3.6.1 SUBTASK 6.1 – PROVIDE COMMUNICATIONS MANAGEMENT

The contractor shall provide communications support to include, but not limited to the following:

- Support all of CB internal communications, including: identifying, developing, facilitating and reviewing content for Brown Bags/presentations/briefings, maintaining an events calendar, developing agendas and briefing materials for presentations (i.e. All

Hands), developing and promoting spirit days and team building events, and drafting, reviewing and editing internal memos for staffing.

- Support the government in developing, implementing and executing program level communications plans that shall address both formal and information communication channels **(Deliverable 28)**. The Communications Plan shall define frequency and types of communications, and necessary communications processes and procedures to ensure efficient and effective flow of information. The communications plan shall implement and evaluate the effectiveness of communications/outreach tactics among the target audience.
- Develop and maintain 101 decks for branches, outlining the functions of the organization and how it supports the Cybersecurity Division's portfolio and agency customers.
- Maintain approved templates, CISA style guide and updates, and perform technical edits on documents as needed.
- Develop communications strategies, stakeholder strategies, work plans and associated communications and messaging materials for CISA cybersecurity programs as well as CB sub-divisions.
    - Work collaboratively with all stakeholders to ensure all materials have a consistent message and program "branding"
    - Develop key messaging and materials for target audiences.
- Develop fact sheets supporting programs and other collateral materials.
- Identify key metrics to measure CISA cybersecurity program successes and gaps. The contractor shall collect and analyze information provided by internal and external stakeholders (e.g. CDM stakeholders) to document metrics, and prepare and distribute associated reports, graphics, spreadsheets, presentations, and talking points to CISA or other stakeholder audiences (e.g. participating agencies, OMB, CB vendors), as appropriate to increase awareness of program status and successes.
- Support development and messaging of program strategies, service capability roadmaps, milestones, talking points, briefings, and timelines to address federal cybersecurity needs. Topics include, but are not limited to AWARE, Dashboard, Shared Services, HVAs, etc.
- Develop and support workshops and or working groups in support of Capacity Building Sub-Division's mission and authorities including but not limited to: CyberStat, FISMA, AWARE, LOE4, FEIT, etc.
- Draft action plans **(Deliverable 34)** that demonstrate how service readiness activities will be executed in coordination with CISA programs and services.
- Develop and provide presentation materials **(Deliverable 2)** and collect meeting minutes **(Deliverable 4).**
- Develop concept of operations plans (CONOPs) **(Deliverable 29)** and other program level documentation in support of CB Sub-Divisions mission and authority that define the roles and responsibilities of CISA and customer agencies in identifying, detecting, and monitoring applications in a pre-operational (production) environment.

3.6.2 SUBTASK 6.2 – PROVIDE WEBSITE MANAGEMENT

The contractor shall develop and/or monitor, explore, and update each CB branches web presence. The contractor shall ensure external content is up to date, monitored and maintained. The contractor shall interact with appropriate stakeholders (i.e. CISA External Affairs, etc.) to obtain content approval. The contractor shall explore social media outlets and others mean to promote the Capacity Building Sub-Division (develop videos, etc.).

3.6.3 SUBTASK 6.3 – PROVIDE GRAPHIC DESIGN

The contractor shall develop and design graphics. Graphics include producing wall posters, fact sheets, grouping cards, newsletters, video images, slides, briefings, etc. The contractor shall support communications activities by producing graphics to visually illustrate capabilities and mission of CB branches and programs.

3.6.4 SUBTASK 6.4 – PROVIDE VIDEOGRAPHER & EDITOR SUPPORT

The contractor shall provide videographer and editor support to include, but not limited to the following:

- Shoot footage and edit the footage into a completed video
- Accomplish the bulk of the technical tasks related to pre-production, production, and post-production
- Work closely with the internal client to formulate and execute the video content and concept through to completion.

3.6.5 SUBTASK 6.5 – PROVIDE EVENT MANAGEMENT

The contractor shall provide event management to include, but not limited to the following:

- Customer mission engagement, operations planning and support for CB Sub-Division stakeholder and industry engagement. Support customer events, meetings and engagements via collaboration with agencies to share information related to development progress, as well as best practices and lessons learned that might benefit all agencies. The contractor shall provide stakeholder outreach and relationship management services that effectively facilitate communications regarding programs to include but not limited to: working groups, events management, marketing, etc. Stakeholder activities include but are not limited to:
    - Customer Advisory Forums (CAFs), AWARE Working Groups, etc.
    - Vendor Engagement Briefings
    - Leadership meetings (e.g. SMAC, CIO/CISO Council, CPASS, FCAC)
    - Support of Federal Cyber Risk Administrator (FCRA) buildout and stakeholder coordination.
- Create agendas, presentation materials, talking points, correspondence, distribution lists, assist in establishing charters and gathering metrics, and facilitate meetings. The contractor shall participate in stakeholder engagement meetings, and document minutes and action items for both internal and external stakeholder groups, including Cybersecurity program customer agencies. The contractor should develop and execute surveys in support of engagements.

- Support media and speaking engagements. That contractor shall liase with CISA EA and venues, draft presentations, write speeches, create talking points, and public affairs materials for DHS CISA CSD's cybersecurity programs and services.
- Identify, track and coordinate involvement in cybersecurity government and industry events.

3.6.6 SUBTASK 6.6 – PROVIDE TECHNICAL WRITER/EDITOR SUPPORT

The contractor shall provide technical write and editor support to includes, but not limited to the following:

- Assist authors or subject matter experts to improve written materials and documents focused on consistency, clarity, and succinctness as well as sentence structure, grammar, spelling, and punctuation
- Analyze and edit both draft and final versions of a variety of acquisition and technical papers
- Advise authors of options and alternatives on the selection, arrangement, form, and content of the end product
- Discuss presentation and revisions with the author prior to finalizing the documents to ensure technical accuracy and that the selection and presentation of information is consistent with the purpose of the publication and its intended audience
- Follow publications through life-cycle development.

3.6.7 SUBTASK 6.7 – PROVIDE COMMUNICATIONS AND OUTREACH SUPPORT (OPTIONAL)

The contractor shall expand and/or surge support to 3.6.1 Subtask 6.1 – Provide Communications Management, 3.6.2 Subtask 6.2 – Provide Website Management, 3.6.3 Subtask 6.3 – Provide Graphic Design, 3.6.4 Subtask 6.4 – Provide Videographer & Editor Support, 3.6.5 Subtask 6.5 – Provide Event Management, and 3.6.6 Subtask 6.6 – Provide Technical Writer/Editor Support as CB mission and priorities expand and evolve.

3.7 TASK 7 – PROVIDE ADMINISTRATIVE AND KNOWLEDGE MANAGEMENT SUPPORT

The Contractor shall assist the Government in the day-to-day coordination of mission support and office operations necessary to support CB and programs including office management activities, information technology support, training, emergency planning, files management, and administrative support.

3.7.1 SUBTASK 7.1 – PROVIDE EXECUTIVE ASSISTANT AND ADMINISTRATIVE SUPPORT

The contractor shall provide administrative, programmatic, and advisor support to CB Leadership. The contractor shall provide executive assistance support to include, but not limited to the following:

- Provide calendar management, scheduling assistance and meeting requests to senior staff members. The contractor shall deconflict calendars as needed and be pro-active in reserving meeting times and reaching out to meeting participants for availability.
- Reserve meeting space, schedule conference rooms and teleconferences/Teams meetings as necessary;
- Provide administrative and logistical support, including pre-meeting coordination and post-meeting follow-up, to support participation for meetings and events, including international engagements, committee meetings, workshops and/forums or working groups
- Support meeting logistics support for on-site events (including activities such as coordinating teleconferences, video teleconferences, meeting registration, meeting sign-in, materials production, visitor escort and registration, room reservations, off-site meeting venue research as needed, note taking, among other related activities)
- Assist in the preparing correspondence, briefing materials, reports, and other related documentation in support of Division/Sub-Division activities;
- Draft support documentation as necessary to support the continued success and sustainment of business operations, including but not limited to SOPs, templates, analyst guides, training documentation, product catalogues, metadata processes and procedures, metadata, etc.
- Perform official travel arrangements and prepare vouches upon Government return from travel. All arrangements shall be made in the CONCUR System. These duties include providing subject matter expertise and advisement the federal travel regulations as it relates to their trip. The contractor shall assist the Government in monitoring and tracking travel requests from initiation through close-out and draft and submit all necessary documentation.
- Assist the Government with emergency planning and continuity of operations preparedness.
- Collaborate with the Division/Sub-Division staff in coordinating responses to and in support of administrative activities as defined by the program. This includes coordinating response to non-budget taskers.
- Advise and assist in the development of standardized office policies, processes, and procedures, as well as facilitate the execution.
- Track and manage Government office floor space planning efforts and coordination support including but not limited to: office logistics planning, including space/facilities planning for offices and geographically dispersed employees, seat reservation management emergency preparedness and new employee orientation.
- Support the government with visitor access requests, making arrangements to obtain clearance for the visitor through the Security Office and advising office visitors of security procedures in advance of their visit. This support shall include escorting responsibilities.
- Monitor, track and organize Government office supplies and inventory. Identify when supplies are low, research and draft orders to replenish and order additional supplies,

reach out to SD/Branches on requests for supplies and ensure supplies are delivered to appropriate stakeholders.
- Perform data entry as needed
- Assist in responding to periodic and ad hoc requests for information.

3.7.2 SUBTASK 7.2 – PROVIDE HUMAN CAPITAL AND MANPOWER SUPPORT

The contractor shall assist the Government in providing human capital and manpower support to include, but not limited to the following:

- Assist hiring managers in developing job announcements/prepare recruitment packages.
- Support the distribution of ranking/certification lists and resumes to supervisor for possible candidate selection.
- Assist hiring managers in developing SNA/QA memos for approval.
- Assist CSD HC in preparing applications for qualification
- Support the submission of promotions, resignations, reassignments, etc.
- Support reporting requirements (e.g., vacancy, hiring status) to the branches and support reporting requirements passed down by CISA OCHCO or CSD Front Office.
- Support the preparation, submission, and tracking of all SLRP and training requirements.
- Support onboarding activities of new federal hires (i.e. order and track IT equipment, seating, phones, etc.).

3.7.3 SUBTASK 7.3 – PERFORM MAILBOX/DISTRO MANAGEMENT

The contractor shall perform mailbox management for the Capacity Building Sub-Division and Branches. Mailbox management includes monitoring email traffic, responding to emails as appropriate, managing and updating distribution lists, and managing access for group mailboxes per governmental guidance. The contractor shall ensure email communication in each program's mailbox is managed appropriately to support its established function and ensure customer inquiries are addressed in a timely fashion.

3.7.4 SUBTASK 7.4 – PROVIDE EXECUTIVE SECRETARIAT SUPPORT

The contractor shall provide executive secretariat support to assist the Government in helping to develop strategic guidance, internal procedures and policies for operations, and executive secretariat initiatives similar to a Director's Action Group to support the overall CSD mission. The contractor shall assist the Government with providing executive secretariat support to include, but is not limited to the following:

- Coordinating and managing of information (e.g., reporting, staffing meetings, supporting project management efforts) for cross-CB strategic and priority initiatives. The contractor shall work with divisions within CSD and across CSD on tasks related to cybersecurity to ensure a timely coordinated response.
- Consolidating, assigning, and tracking action items on behalf of CB Associate Director (A/D) and CB Deputy A/D. The contractor shall track and report on general status of tasks directed by DHS/CISA/CSD/CB leadership, to include timelines and milestones for completion. The contractor shall develop, maintain and update a Task Tracker Report **(Deliverable 35).** The contractor shall ensure leadership is aware of timelines and

milestones for task completion and is aware of and understands issues that may arise as a result of suspense.

- Support the development, management, and execution of CB-wide program management reviews.
- Development and coordination of short, medium, and long-range strategy and/or strategic planning efforts and artifacts to support the growth and evolution of Capacity Building.
- Develop and execute a wide range of strategic, programmatic, and tactical support to establish and maintain organizational tools and operations that support organization wide initiatives.
- Development and coordination of standardized, repeatable, and automated (as much as possible) CB-wide daily/weekly reporting efforts. The contractor shall assist the Government in developing and implement procedures and plans for improvements and enhancements pertaining to office best business practices.
- Monitor and measure staff requirements, operations, and productivity patterns to identify opportunities for process improvement in order to maximize efficiency.
- Technical writing, editing and quality assurance support for tasks directed by DHS/CISA/CSD/CB leadership.
- Prepare presentation slide decks, talking points, maintain plan(s), maintain documentation and files, and assist in the scheduling of events as needed.

3.7.5 SUBTASK 7.5 – PROVIDE RECORDS MANAGEMENT

The contractor shall assist the Government by providing records management to include, but not limited to the following support:

- Subject matter expertise with regards to the operations of the Records Management program in the CSD mission areas as implemented and directed by the DHS Records Management Program, CISA Records Management Program, and in accordance with National Archives and Records Administration (NARA) guidelines. Support shall include, but not limited to:
    - Administrative support of the program, such as metrics tracking and weekly/monthly reporting, task management functions, records management requirements, SOP/guidance documents development and update, etc.
- Perform records analysis support to include providing file plan management support, disposition support, etc. in conjunction with CISA Records Management Program requirements and tasks.
- Support current records management tools, identify and recommend new records management tools to leverage. Documents are currently tracked in SharePoint 2016.
- Provide logistical and administrative support to CSD Records Management working groups, draft as necessary any guidance documents for the CSD Records Management Office Liaisons and Records Custodians, coordinate closely with the CISA Records Management Office to advocate for CSD ‘s record management needs and priorities.
- Develop a standard document naming convention to govern the way files are titled across CSD. After the establishment of a standardized records management structure, the

contractor shall assist the CISA Records Liaison in promoting compliance across CSD through regular communications, advice and other supports services as necessary.

3.7.6 SUBTASK 7.6 – PROVIDE HUMAN RESOURCES SUPPORT

The contractor shall assist the Government in providing human resources support to include, but not limited to the following:

- Establish and implement training processes and procedures and coordinate training request packages
- Develop templates and workflows to simplify the training application and approval process for Federal employees
- Ensure staff training requirements and requests are met. Typically, on an annual basis.
- Provide communications and outreach to bring awareness to training opportunities
- Identify, coordinate and organize group trainings for sub-division/branch staff
- Establish and implement a Awards and Recognition Program
- Coordinate and consolidate award submissions for all DHS (to include CISA, CSD, CB) Award and recognition opportunities. The contractor shall recommend ways and work to streamline the awards nomination and submission process
- Develop tailored professional development roadmaps for the sub-division and staff
- Develop and provide useful and helpful resources, to include templates, communications, etc. for staff to leverage to inform them of professional development opportunities
- Coordinate with CISA and CSD to support the communications and outreach to bring awareness to professional development opportunities and support.

3.7.7 SUBTASK 7.7 – PROVIDE KNOWLEDGE MANAGEMENT

CB's intellectual capital, the knowledge that people gain through experience, if made accessible to CB personnel, will minimize "reinventing the wheel" and ultimately reduce costs to the taxpayer; therefore, it is the intention of the Government to use Knowledge Management (KM) to develop and improve mission control, efficiency, and effectiveness. The contractor shall assist the Government in providing knowledge management to include, but not limited to the following:

- Develop and support a knowledge management strategy **(Deliverable 36)** for CB and its branches to include SharePoint, OneDrive, MS Teams, and other applicable CISA applications and areas of web presence.
    - Once approved, the contractor shall facilitate the execution of the knowledge management strategy.
- Develop of strategic guidance, repeatable processes, management and facilitation of policies and procedures resulting in sound business management, to include automation where applicable.
- Document and maintain knowledge management repositories to include, but not be limited by internal SOPs, assessment scheduling and prioritization processes, and other process improvements pertaining to the Service Desk
- Update and distribute recurrent reports/metrics as needed by the government

- Establish, maintain and update central libraries/repositories for CISA/CB programs. The contractor shall work to develop a standard document management system to support the development of guidance documents. The contractor shall establish criterion to determine what level of review and approval is required for documents published through the program. The contractor shall establish a repeatable and transferable process that will include specific review and control gates by appropriate levels of leadership. These libraries include, but are not limited to, repositories for:
    - CISA cybersecurity programs using CISA systems and tools
    - CB sub-division PMO-specific communications and stakeholder engagement materials, including slide repositories.

3.7.8 SUBTASK 7.8 – PROVIDE SHAREPOINT/MICROSOFT O365/TOOLS AND PORTALS SUPPORT

The contractor shall provide SharePoint/O365/Tools and Portal support to include, but not limited to the following:

- Support Sharepoint development, updates and administration to include but not limited to the following:
    - Manage CB wide permissions and Sharepoint groups;
    - Trouble-shoot Sharepoint permission issues;
    - Manage Sharepoint content data and crate new database as required;
    - Provide technical support on Sharepoint solutions as required, including creating and manipulating web-parts and creating new Sharepoint pages and sites;
    - Consolidate information and draft responses to taskers as required
- Provide a SharePoint subject matter expertise to maintain documents, calendars, checklists, workflows and permissions, including to the training staff, Action Officers and Executive Secretary (Exec-Sec) personnel. In addition, make recommendations for improved portal and website communications
- Microsoft (MS) O365 subject matter expertise to study the current use of MS O365 products and services and assist in the implementation of best practices to increase effectiveness and efficiency of Division/Sub-Division processes
- Assist with maintaining document repositories, calendars, checklists, workflows and permissions in a O365 environment.

3.7.9 SUBTASK 7.9 – PERFORM CONTRACTOR MANPOWER DATABASE MANAGEMENT AND EOD TRACKING

CB's contractor manpower database and EOD tracking provides a clear accounting of all CB contractor personnel and their security status. The contractor manpower database tracks and reports status and makes the data accessible at any given time providing an up to date and immediate understanding of CB's contractor footprint, security status and overall contractor portfolio. The contractor shall assist the Government in performing contractor manpower database management and EOD tracking to include, but not limited to the following:

- Monitor the CSD CB Contractor Security Mailbox on a daily basis (csd_cb.contractorsecurity@cisa.dhs.gov) in line with the current Contractor Security

Mailbox SOP. This includes review and follow-up of all received correspondence to ensure actionable items are completed.

- Develop guidance, repeatable processes, management and facilitation of policies and procedures related to the contractor manpower database management and EOD tracking.
- Document, maintain, and distribute the following:
    - Weekly Change Log
    - Contractor Security Bi-Weekly Report
    - Daily Status Updates
    - Staffing Plans
- Review and analyze reports and provide daily updates on EOD statuses and disseminate to the appropriate CORs as outlined by the government.
- Maintain the data within the database and ensure accurate and up to date information is captured within for each contractor.
- Liaise with the security office(s) tracking and reporting on EOD status.
- Update and distribute recurrent reports/metrics as needed by the government.
- Attend, and lead meetings related to the status of the Contractor Manpower Database and associated information.

3.7.10 SUBTASK 7.10 – PROVIDE ADMINISTRATIVE AND KNOWLEDGE MANAGEMENT SUPPORT (OPTIONAL)

The contractor shall expand and/or surge support to all of the Task 7 activities identified above as CB mission and priorities expand and evolve.

3.8 TASK 8 – PROVIDE GOVERNANCE AND POLICY SUPPORT

CISA, through its directives authority, is responsible for establishing federal policy related to operational cybersecurity and emergent vulnerabilities and threats. Additionally, CISA supports Federal civilian agencies in understanding, adopting, and implementing cybersecurity policies and priorities set by the White House. This support includes developing implementation guidance, directly engaging, and driving accountability and compliance with policy requirements.

Within an agency, CISA promotes effective cybersecurity governance practices through the provision of governance-focused planning support, technical assistance services, and products to fill any governance gaps identified. CISA also seeks to advance agency organizational readiness and federal enterprise adoption of capacity building tools and services offered by and/or through capacity building programs to mitigate emerging threats and risks. The Government requires contractor support to provide governance and policy support.

3.8.1 SUBTASK 8.1 – PROVIDE GOVERNANCE AND POLICY SUPPORT

On the heels of recent cyber-attack campaigns, CISA has begun building a cross-functional team charged with assessing agency capabilities and limitations, developing tailored cybersecurity improvement plans, and increasing direct engagement with agencies and across the federal enterprise.

The contractor shall assist the Government in providing the following governance and policy to include, but not limited to include the following:

- Develop content for cybersecurity directives (i.e. Binding Operational Directives (BODs), Executive Orders (EOs), etc.) and guidance to meet mandates and requirements.
- Analyze existing policies, directives, and guidance to assist in the development of federal enterprise-wide priorities and implementation plans.
- Develop agency-specific cyber risk and capability profiles and cybersecurity improvement plans leveraging data and information gathered by CISA through assessments, performance measurement, and operational activities.
- Assist in monitoring and tracking agency compliance with policies and directives.
- Develop cybersecurity implementation and improvement guidance, templates, and sample programmatic resources (e.g., policies, procedures, use cases) across a variety of cyber domain areas.
- Assist in interacting with agency representatives, both technical and leadership, to support their remediation and improvement efforts in both collective (e.g., workshop, Q&A session) and individual settings.
- Identify potential CISA services/products/offerings that can assist agencies with remediation and improvement efforts.

3.8.2 SUBTASK 8.2 – PROVIDE GOVERNANCE AND POLICY SUPPORT (OPTIONAL)

The contractor shall expand and/or surge support to 3.8.1 Subtask 8.1 – Provide Governance and Policy Suppor as CB mission and priorities expand and evolve.

3.9 TASK 9 – PROVIDE PROJECT TRACKING/ORDER MANAGEMENT SUPPORT

Acquisition and Budget (AB) enhances CB subdivisions and its customer agencies by leading full lifecycle acquisition and establishing innovative acquisition solutions. AB fosters partnership and collaboration with industry and customer agencies to lead and deliver complex, large scale cybersecurity acquisitions, budget, and project management activities on behalf of CB. Support includes researching, developing, and managing innovative information technology (IT) acquisition and contract strategies, providing oversight, review, and approval of contract deliverables, and manage contract operations and performance by ensuring contractors deliver high-quality solutions on time, and leading pre-award and post-award acquisition tasks and requirements development to create flexible, fast, and cost-effective vehicles.

The contractor shall assist the Government in providing acquisition and procurement management focused on project tracking and order management to assist in planning, coordinating, and tracking activities in support of Acquisition and Budget.

3.9.1 SUBTASK 9.1 – PERFORM PRE-AWARD SUPPORT

The contractor shall assist the government with the pre-award functions associated with awarding new contracts, task orders, agreements, and financial transfers, including procurement planning, advising, and assisting the government regarding contract or task order issues

involving scope and compliance. The contractor shall assist the Government in providing direct acquisition and procurement support to assist in developing and executing acquisition strategies and developing acquisition documents. The contractor shall provide subject matter expertise to assist the Government in providing quality acquisitions that lead to improved resource utilization, smooth transitions, and successful post-award solutions.

The contractor shall support the government in analyzing acquisition policies, plans and procedures. The contractor shall assist the government in procurement forecasting, acquisition planning and strategy, status updates, and memos for record. Activities include, but are not limited to:

- Assist in acquisition strategy development and support
    - Acquisition and procurement forecasting and planned activities
    - Acquisition policy research and organizational planning
    - Develop innovative contract approaches
- Conduct market research
    - Draft RFI content and perform RFI analysis
    - Conduct other forms of research to include:
        - Commercial and marketplace offerings
        - Pricing and segmentation analysis
        - Supply chain
- Develop acquisition plans
- Conduct requirements gathering
- Provide input to Government cost estimates
    - Research historical data
    - Perform pricing research
    - Develop cost strategies that result in government cost savings
- Conduct procurement planning and scope advisory assistance support
- Draft procurement documentation such as SOWs, PWSs, PRs, required justifications, determinations and findings for government review and approval
- Perform technical writing, editing, and quality assurance support
- Draft and track schedules for procurements in the pre-award phase
- Facilitate and plan industry events: industry days, due diligence sessions, etc.

3.9.2 SUBTASK 9.2 – PERFORM POST-AWARD SUPPORT

The contractor shall assist the Government in performing post-award contract management support to include, but not limited to the following:

- Maintaining COR files ensuring files are current and complete.
- Participate in team meetings, program management reviews, and other related meetings.
- Monitor contract financial status. The contractor shall assist in tracking financials, via Excel spreadsheets, to include obligations and expenditures for multiple IAAs; modifications; burn rates; funding exhaustion dates; funding expiration dates. The contractor shall assist in liaising with Agencies and providing funding updates.

- Assist with the coordination of inspection and acceptance or rejection of deliverables. The contractor shall develop/maintain a deliverable status tracker for each contract/TO. The contractor shall take lead on managing the review process for documents and deliverables to include ensuring prompt review of deliverables by the team and provide recommendations for approval/disapproval/comments.
- Assist in performance management. For award fee type contracts, the contractor shall assist coordinating the process for mid-term and final reviews. The contractor shall solicit feedback from performance monitors and award fee board personnel. The contractor shall assist in coordinating feedback sessions and board meetings.
- Provide analyses when changes to existing support concepts are anticipated. These analyses shall include recommendations to enable the Government to make informed decisions.
- Perform evaluations of recommendations for contractor change proposals and related documents.
- Provide cybersecurity subject matter expertise to Capacity Building Service Management to ensure procurement and configuration elements adequately address Federal user needs.
- Provide support and coordination to CORs in executing key activities in support of the execution of cybersecurity solutions (i.e. execution of OMB memorandums)
- Assist in the administration and management of the shared services platform. The contractor shall support the management of the DEFEND Portfolio Groups, monitoring/tracking Requests for Services (RFSs) and updating their status at an enterprise level and drafting, reviewing, and editing RFSs and capability statements as required by government direction. The contractor shall capture lessons learned and apply them to the development and management of RFSs across the RFS Lifecycle. **(Deliverable 20)**
- Assist in contract tracking efforts by developing and maintaining documentation related to the execution of the CB SD's shared services platforms and acquisition efforts, including service/capability contract awards, manpower estimates and weekly Capacity Building Sub-Division contract management meetings **(Deliverable 37).**
    - The contractor shall maintain and make enhancements to the existing Purchase Request (PR) File Management system, tracking and reporting on all executed contractual actions on the shared services platform for the program office.
    - The contractor shall assist CORs in tracking status and maintaining documentation related to shared services PRs from inception to award and assist CORs in determining when follow-on actions are anticipated and/or required. The contractor shall prepare and maintain reports and dashboards relaying the status of PR actions **(Deliverable 35).**
- Provide support and assistance to the government in preparing IT acquisition review (ITAR) Checklists and briefings and adjudicating and DHS CIO review comments and tracking approval.
- Prepare of the Balance Workforce Strategy (BWS), including but not limited to the area of cost analysis.

- Assist CORs with contract closeout tasks.

3.9.3 SUBTASK 9.3 – PROVIDE STRATEGIC PORTFOLIO SUPPORT

The contractor shall assist in establishing processes and best practices to ensure sound contract management and ensure government is a leader in cybersecurity acquisition. Additionally, the contractor shall provide contract management support to AB and other CB organizations. The contractor shall assist the Government in providing strategic portfolio support to include, but not limited to the following:

- Assist in the development of strategic guidance, repeatable processes, management and facilitation of acquisition procedures and policies resulting in quality contract management.
- Assist in the development of advanced contract management solution(s) to assist the Government in not just managing contracts effectively but also developing seamless processes and workflows to achieve excellence.
- Develop and provide configuration control and database management in support of contracts management.
- Assist with the development of standards and the analysis of best practices, lessons learned to provide efficiencies
- Establish and update a repository for contract artifacts, best practices, and standard operating procedures
- Strategize to develop and build-out acquisition business processes, and establish a Center of Excellence
- Establish and implement quality and process improvement
- Establish and develop acquisition templates for all types of contract support activity to allow for a streamlined procurement development and planning activities
- Assist with developing advanced contract management solutions to include, but not limited to the following
- Assist in developing an external communications strategy showcasing CB’s acquisition offerings in a marketplace, web presence or other means increasing visibility, awareness and communication of offerings.
- Develop a process to seamlessly and continually capture and manage contract related metrics; develop contract and portfolio performance metrics as they relate to successful mission objectives of CB
- Provide enterprise view and reporting on contract execution activities
- Prepare and develop content for presentations, slide decks, talking points, maintain plan(s), maintain documentation and files, and assist in the scheduling of events as needed
- Ensure leadership is aware of timelines and milestones for task completion and is aware of and understands issues that may arise as a result of suspense

3.9.4 SUBTASK 9.4 – PROVIDE PROJECT TRACKING/ORDER MANAGEMENT SUPPORT (OPTIONAL)

The contractor shall expand and/or surge support to all of the Task 9 activities identified above as CB mission and priorities expand and evolve.

4.0 QUALITY ASSURANCE AND ACCEPTABLE CRITERIA

The Government will establish and maintain a Quality Assurance Surveillance Plan (QASP) for work accomplished under this contract. The QASP will be based under the following standards and acceptable quality levels (AQL)s:

Std #	PWS Ref	Performance Standard	Acceptable Quality Level
			•
			•
			•
			•
			•
			•
			•
			•
			•
			•
			•
			•

5.0 CONTRACT DELIVERABLES

The following abbreviations are used in this schedule:

DEL: Deliverable

All references to days: Government Workdays

Deliverables are due the next Government workday if the due date falls on a holiday or weekend.

The service provider shall deliver the deliverables listed in the following table on the dates specified:

Del #	Deliverable	Contract Reference	Due Date
1	Agenda	3.1.1	5 business days prior to meeting
2	Presentation Materials	3.1.1	As required
3	Monthly Status Briefing	3.1.2	10th calendar day of the month
4	Meeting Minutes	3.1.2	1 business day following meeting
5	Trip Reports	3.1.2	5 business days after trip
6	Problem Notification Reports	3.1.2	1 business day after identification of problem
7	Draft PMP	3.1.3	14 calendar days after TOA
8	Final PMP	3.1.3	30 calendar days after kick-off meeting
9	Quality Control Plan	3.1.4.1	Draft delivered 14 calendar days after TOA Updates made as requested by the Government
10	Transition In Plan	3.1.5.1	14 calendar days after TOA
11	Transition Out Plan	3.1.5.2	90 calendar days prior to TO expiration
12	Financial Report	3.1.6	10th calendar day of the month
13	In-Progress Review Briefing	3.1.8	Quarterly
14	Risk Tracker	3.2.1.1, 3.2.2.1, 3.2.4	As required
15	Capabilities Roadmap	3.2.1.1, 3.2.3	As required
16	Quad Charts	3.2.1.1	As required
17	Weekly Report	3.2.1.1	As required
18	Process/Procedure Documentation	3.2.1.1, 3.2.2.3, 3.2.2.5, 3.2.2.8,3.2.7.1, 3.4.1, 3.4.2, 3.4.3	As required
19	Agency Capability Schedule	3.2.2.1	As required
20	Lessons Learned Repository	3.2.2.1, 3.9.2	As required
21	Project Plans	3.2.2.3	As required
22	Service Delivery Plans	3.2.2.4	As required
23	Analysis of Alternatives	3.2.2.4	As required
24	Business Case Development	3.2.2.8	As required
25	Strategic Plan	3.2.2.8, 3.2.3	As required

26	Improvement Plans	3.2.2.8, 3.2.7.2, 3.4.1	As required
27	HVA System Profile Management	3.2.4	As required
28	Communication Plan	3.2.7.1, 3.6.1	As required
29	Program Strategy Documentation	3.3.1, 3.6.1	As required
30	Metrics	3.4.1	As required
31	Product Workbook	3.4.1	As required
32	RIP Tracker	3.4.2	As required
33	Forecasting Reports	3.4.3	As required
34	Action Plans	3.6.1	As required
35	Task Tracker	3.7.4, 3.9.2	As required
36	Knowledge Management Strategy	3.7.7	As required
37	Document Repository	3.9.2	As required

6.0 TRAVEL

6.1 TRAVEL REGULATIONS

Contractor costs for travel will be reimbursed at the limits set in the following regulations (see FAR 31.205-46):

a. FTR - prescribed by the GSA, for travel in the contiguous U.S.
b. DSSR (Government Civilians, Foreign Areas), Section 925, "Maximum Travel Per Diem Allowances for Foreign Areas" - prescribed by the Department of State, for travel in areas not covered in the FTR.

6.2 TRAVEL AUTHORIZATION REQUESTS (TAR)

Before undertaking travel to any Government site or any other site in performance of this TO, the contractor shall have this travel and coordinated with the CISA Functional Lead and approved by the COR. Notification shall include, at a minimum, the number of persons in the party, traveler name, destination, duration of stay, purpose, and estimated cost. Prior to any long distance travel, the contractor shall prepare a TAR **(Attachment G – TAR)** for Government review and approval. Long distance travel will be reimbursed for cost of travel comparable with the FTR and DSSR.

Requests for travel approval shall:

a. Be prepared in a legible manner.
b. Include a tracking ID number
c. Include a description of the travel proposed including a statement as to purpose
d. Be summarized by traveler.
e. Identify the TO number.
f. Identify the CLIN associated with the travel.
g. Be submitted in advance of the travel with sufficient time to permit review and approval.

The contractor shall use only the minimum number of travelers and rental cars needed to accomplish the task(s). Travel shall be scheduled during normal duty hours whenever possible.

7.0 ROLES AND RESPONSIBILITIES

Identification of all government personnel, including their specific roles and responsibilities:

7.1 CONTRACTING OFFICER

xxxxxx GSA FAS
Telephone Number:
Electronic Mail:

Responsibility for contracting activities rests solely with the Government Contracting Officer. No conversation, recommendations, or direction, whether given directly by, or implied by Government personnel, that will affect the scope, schedule, or price of the program covered by this solicitation or any resulting contract, shall be acted upon by the Contractor unless specifically approved by the Government Contracting Officer. In the absence of the assigned CO, any GSA Region 8 CO may fill in and has full authority to act on this task order.

7.2 CONTRACTING SPECIALIST

xxxxxx GSA FAS
Telephone Number:

Electronic Mail:

As a member of the contract administration team, the contract specialist will be responsible for working in concert with the Contracting Officer while performing post award administrative functions and certain assigned pre-award functions.

7.3 CONTRACTING OFFICER'S REPRESENTATIVE (COR)

TBD, DHS
Telephone Number: TBD
Electronic Mail: TBD

CONTRACTING OFFICER'S REPRESENTATIVE (DEC 1991)

(a) Definition. "Contracting officer's representative" means an individual designated in accordance with subsection 201.602-2 of the Defense Federal Acquisition Regulation Supplement and authorized in writing by the contracting officer to perform specific technical or administrative functions.

(b) If the Contracting Officer designates a contracting officer's representative (COR), the Contractor will receive a copy of the written designation. It will specify the extent of the COR's authority to act on behalf of the contracting officer. The COR is not authorized to make any commitments or changes that will affect price, quality, quantity, delivery, or any other term or condition of the contract.

8.0 PLACE OF PERFORMANCE/PERIOD OF PERFORMANCE

The primary place(s) of performance at Task Order Award (TOA) is at contractor's facility due to the current circumstances of the national pandemic.

During the PoP of the TO and as the workplace circumstances evolve the contractor shall perform the TO requirements on-site at the government's facility located in Ballston, VA and off-site at the contractor facility. An on-site support schedule will be identified post-award. It is preferred that the contractor's facility be within the Washington DC metro area/NCR and near the Government's location in Arlington, VA (Ballston area). The contractor shall be required to routinely travel to the to the Government's location in Arlington, VA (Ballston area). All access to classified information will only take place at Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) U.S. government locations in the greater Washington, DC metropolitan area. The contractor's facility shall include conference and meeting room space and support routine Government meetings and events. The contractor shall provide support during normal operating hours from 0800 to 1700 daily, five (5) days a week (Monday through Friday).

Period of Performance

Base Period	12 mo	TBD	TBD
Option Period 1	12 mo	TBD	TBD
Option Period 2	12 mo	TBD	TBD
Option Period 3	12 mo	TBD	TBD
Option Period 4	12 mo	TBD	TBD

9.0 OTHER DIRECT COSTS (ODCS)

ODC include costs associated with facilities to accomplish training tasks, as well as infrastructure that will assist in delivery of support. ODCs will be reimbursed at cost.

10.0 GOVERNMENT-FURNISHED EQUIPMENT (GFE) AND GOVERNMENT FURNISHED INFORMATION (GFE/GFI)

The Government will provide onsite/offsite contractors with laptops, cellular phones and access to DHS computer network, as necessary.

Use of GFP offsite shall be in accordance with FAR part 45 and the contractor will be responsible and liable for GFP pursuant to FAR 52.245-2, 52.245-5, and HSAR 3052.245-70 as applicable. Pursuant to HSAR 3052.245-70, all GFP used offsite shall be documented and included in annual reports using DHS Form 0700-5, Contractor Report of Government Property. The contractor shall return GFP used offsite to Government specified locations. The contractor will be responsible for providing office space, supplies, telecommunications, and equipment for work performed at its facilities.

The Government will provide all necessary information, data and documents to the contractor for work required under this contract. The contractor shall use Government furnished information,

data and documents only for the performance of work under this contract and shall be responsible for returning all Government furnished information, data and documents to the Government at the end of the performance period. The contractor shall not release Government furnished information, data and documents to outside parties without the prior written consent of the CO.

10.1 GOVERNMENT-FURNISHED INFORMATION (GFI)

The contractor shall protect all GFI (e.g., Government data) by treating the information as Sensitive But Unclassified (SBU). SBU information and data shall only be disclosed to authorized-personnel as described in the TO herein. The contractor shall keep the information confidential and use appropriate safeguards to maintain its security in accordance with minimum Federal standards.

When no longer required, this information and data shall be returned to Government control, destroyed, or held until otherwise directed by the GSA CO. The contractor shall destroy unneeded items by burning, shredding, or any other method that precludes the reconstruction of the material.

If work under this TO requires that the contractor's personnel have access to Privacy Information, contractor personnel shall adhere to the Privacy Act, Title 5 of the U.S. Code, section 552a and applicable Agency rules and regulations.

11.0 CONFIDENTIALITY OF DATA

The contractor is required to comply with FAR 9.505-4(b), A contractor that gains access to proprietary information of other companies in performing advisory and assistance services for the Government must agree with the other companies to protect their information from unauthorized use or disclosure for as long as it remains proprietary and refrain from using the information for any purpose other than that for which it was furnished. The contracting officer shall obtain copies of these agreements and ensure that they are properly executed. Duplication or disclosure of the data and other information to which the contractor develops or will have access to as a result of this TO is prohibited. It is understood that throughout performance of this TO, the contractor will have access to confidential data, which either is the sole property of the DHS or is the sole property of other than the contracting parties. The contractor and its subcontractor(s) (if any) agree to maintain the confidentiality of all data to which access may be gained throughout task order performance, whether title thereto vests in DHS or otherwise. The contractor and his subcontractor(s) (if any) agree to not disclose said data, any interpretations and/or translations thereof, or data derivative there from, to unauthorized parties in contravention of these provisions, without the prior written approval of the CO and the party in which title thereto is wholly vested. Subcontractors are subject to the same stipulations and may be held responsible for any violations of confidentiality.

12.0 ORGANIZATIONAL CONFLICT OF INTEREST AND NON-DISCLOSURE AGREEMENTS

12.1 ORGANIZATIONAL CONFLICT OF INTEREST

a. If a contractor has performed, is currently performing work, or anticipates performing work that creates or represents an actual or potential OCI, the contractor shall immediately disclose this actual or potential OCI to the CO in accordance with FAR Subpart 9.5. The nature of the OCI may involve the prime contractor, subcontractors of any tier, or teaming partners.
b. The contractor is required to complete and sign an OCI Statement. The contractor must represent either that (1) It is not aware of any facts which create any actual or potential OCI relating to the award of this contract, or (2) It has included information in its proposal, providing all current information bearing on the existence of any actual or potential OCI and has included a mitigation plan in accordance with paragraph (c) below.
c. If the contractor with an actual or potential OCI believes the conflict can be avoided, neutralized, or mitigated, the contractor shall submit a mitigation plan to the Government for review.
d. In addition to the mitigation plan, the CO may require further information from the contractor. The CO will use all information submitted by the contractor and any other relevant information known to GSA, to determine whether an award to the contractor may take place, and whether the mitigation plan adequately avoids, neutralizes, or mitigates the OCI.
e. If any such conflict of interest is found to exist, the CO may determine that the conflict cannot be avoided, neutralized, mitigated, or otherwise resolved to the satisfaction of the Government, and the contractor may be found ineligible for award. Alternatively, the CO may determine that it is otherwise in the best interest of the U.S. to contract with the contractor and include the appropriate provisions to avoid, neutralize, mitigate, or waive such conflict in the contract awarded.

This effort will involve providing professional services assistance and advice, assistance in the preparation of Statements of Work (SOWs) and other acquisition documents, post-award management and access to proprietary and/or sensitive Government and contractor information. The contractor shall be precluded from bidding on any future requirements for which it supported the preparation development of any acquisition documentation. The contractor shall comply with the requirements under FAR Subpart 9.5 Organizational and Teaming/Consultant Conflicts during performance under this TO. The contractor shall recuse itself from any and all future submission of bids, proposals or quotes against all CB and potential CSD solicitations for the duration of this task order and must sign a non-disclosure agreement (NDA).

12.2 NON-DISCLOSURE REQUIREMENTS

If the contractor acts on behalf of, or provides advice with respect to this TO as defined in FAR 3.104-4, then the contractor shall execute and submit a Corporate Non-Disclosure Agreement (NDA) form and ensure that all its personnel (to include subcontractors, teaming partners, and consultants) who will be personally and substantially involved in the performance of the TO:

a. Are instructed in the FAR 3.104 requirements for disclosure, protection, and marking of contractor bid or quote information, or source selection information.

b. Are instructed in Far Part 9 for third-party disclosures when acting in an advisory capacity.

All proposed replacement contractor personnel shall also be instructed in the requirements of FAR 3.104. Any information provided by contractors in the performance of this TO or obtained by the Government is only to be used in the performance of the TO. The contractor shall put in place appropriate procedures for the protection of such information and shall be liable to the Government for any misuse or unauthorized disclosure of such information by its personnel, as defined above.

13.0 CONTRACT TELECOMMUTING-REMOTE PERSONAL RESIDENCE WORK LOCATIONS

Telecommuting for federal government contractors will be allowed to the extent practicable to meet DHS mission needs. Telecommuting allows contractor personnel to perform their contractual requirements outside of CISA office locations, typically at a contractor's personal residence or a corporate telecommuting office location. Telecommuting for contractor personnel provides the government flexibility to meet unique CISA organizational and facility needs and requirements. The goal of telecommuting for contractor personnel is to enhance the delivery of services that support the DHS mission.

Telecommuting is permitted under the task order in accordance with the requirements below.

The COR and the Contractor will mutually agree upon individual contractor's telecommuting schedule. Additionally, the provision to permit contractor telecommuting may be revoked at the Task Order level at any time if the Government makes such determination. The telecommuting provision does not change any task order requirements; all other terms and conditions of the task order remain in full force and effect.

13.1 CONTRACT LABOR RATES WHILE TELECOMMUTING

The contractor shall charge the same applicable fixed hourly rate as for a Government site for those contractor personnel when they telecommute at their designated telecommuting location.

14.0 SECURITY REQUIREMENTS

14.1 GENERAL

The Government requires all information pertaining to this TO be stored and protected in accordance with Government policy regarding SBU information. Therefore, no information shall be stored or transmitted outside the U.S. The information associated with this TO is critical infrastructure information as defined by 1016(e) of the U.S. Patriot Act of 2001 (42 U.S.C. 5195c(e)).

DHS security requirements are also applicable to this TO, including, but not limited to, FAR 52.204-2. In some instances, the contractor shall have to follow specific Agency security requirements that will be provided post-award as GFI.

14.2 FACILITY CLEARANCE LEVEL (FCL)

At the time of proposal submittal, the contractor shall have a contractor facility with an approved facility clearance at the Top Secret (TS) level. Although the TO utilizes information at the SBU level, the FCL will allow for greater classification levels as directed by the Government.

An FCL is an administrative determination that, from a national security standpoint, a facility is eligible for access to classified information at the Confidential, Secret, or TS level. The FCL includes the execution of a DoD Security Agreement (DD Form 441 and DD Form 441-1) and Certificate Pertaining to Foreign Interests (Standard Form (SF) 328). Under the terms of an FCL agreement, the Government agrees to issue the FCL and inform the contractor as to the security classification of information to which the contractor will have access. The contractor, in turn, agrees to abide by the security requirements set forth in the National Industrial Security Program Operating Manual (NISPOM). In general, all necessary FCLs shall be at the expense of the contractor.

14.3. ACCESS TO AND PROTECTION OF CLASSIFIED INFORMATION

The contractor shall ensure these instructions are expressly incorporated into any and all subcontracts or subordinate agreements issued in support of this contract.

Performance on this contract requires the contractor to gain access to classified National Security Information (includes documents and material), which mandates protection in accordance with Executive Order 13526 National Security Information (NSI), as amended, as well as any supplemental directives.

The contractor shall abide by the requirements set forth in the DD Form 254, Contract Security Classification Specification**;** the National Industrial Security Program Operating Manual (NISPOM), as well as any relevant Intelligence Community Directives (ICDs) for protection of classified and/or compartmented information at its cleared facility, if applicable, or as further directed by the Special Security Officer (SSO)/Office of Selective Acquisition Security Manager (OSASM). If the contractor is required to have access to classified information at any DHS or other government facility, it shall abide by the security requirements set forth by the Cognizant Security Authority (CSA) for that facility.

14.4 PERSONNEL SECURITY CLEARANCES

At TOA, only the contractor's PM and DPM contractor personnel shall possess a TS security clearance. The Government will dictate the need for any additional security clearance requirements when applicable.

At a minimum all contractor staff are required to have a Public Trust to obtain DHS Suitability.

In general, all necessary employee security clearances shall be at the expense of the contractor. The contractor shall comply with all security requirements.

14.5 DHS CONTRACTOR SECURITY REQUIREMENTS

14.5.1 HOMELAND SECURITY PRESIDENTIAL DIRECTIVE (HSPD-12)

The contractor shall provide a list of contractor personnel that require DHS badges and security clearances to the DHS COR. The Government will process background investigation and/or security clearances for the contractor staff to occur after submission of the staff listing, provided the individuals meet the necessary security qualifications.

14.5.2 POST-AWARD SECURITY REQUIREMENTS

Contractors requiring access to DHS systems (to include DHS GFP) require personnel security vetting, to include the scheduling and adjudication of the appropriate level of background investigation processed by the DHS Personnel Security Division (PSD). The DHS CDM PMO, in conjunction with the DHS PSD, shall have and exercise full control over granting, denying, withholding, or terminating unescorted Government facility and/or SBU Government information access for contractor employees, based upon the results of a background investigation. Contractor employees assigned to the TO not needing access to SBU Agency information or recurring access to Agency facilities shall not be subject to security suitability screening.

Contractor employees awaiting an Entrance on Duty (EOD) decision may begin work on the TO provided they do not access SBU Government information. Limited access to Government buildings may be allowable prior to the EOD decision if the contractor is escorted by a Government employee. This limited access is to allow contractors to attend briefings, non-recurring meetings, and begin transition work. NOTE: The security process for DHS EOD varies in the length of time it takes to obtain a favorable adjudication. The process is specific to each individual and dependent on their circumstances when their case is submitted. The contractor can assist in expediting the process by being diligent in accurately completing the security paperwork in a timely manner, responding to email, and other questions or requests for information from the security office expeditiously. If the contractor employee has already been granted EOD, at the same level annotated on this contract, under another DHS HQ contract the process for obtaining EOD under this TO will be streamlined.

The contractor shall propose employees whose background offers the best prospect of obtaining a security badge approval for access. Non-U.S. citizens (foreign nationals and/or dual citizenships) are not permitted under this TO.

14.5.3 CONTRACTOR FITNESS DETERMINATION

Access to Government facilities or information at any time during the term of the TO. No employee of the contractor shall be allowed unescorted access to a DHS facility without a favorable EOD decision or suitability determination by the DHS Office of Security/PSD.

The DHS Office of Security/PSD shall be notified of all terminations/resignations within five days of occurrence. The contractor shall return to the CDM COR all DHS-issued identification cards and building passes that have either expired or have been collected from terminated employees. If an identification card or building pass is not available to be returned, a report shall

be submitted to the CDM COR, referencing the pass or card number, name of individual to whom it was issued, and the last known location and disposition of the pass or card.

When sensitive Government information is processed on Department telecommunications and automated information systems, the contractor shall provide for the administrative control of sensitive data being processed. Contractor personnel shall have favorably adjudicated background investigations commensurate with the defined sensitivity level.

Contractors who fail to comply with Department security policy are subject to having their access to Department IT systems and facilities terminated, whether or not the failure results in criminal prosecution. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions under a variety of laws (e.g., Privacy Act).

DHS Security Office POC Information:

Office of Security/PSD Customer Service Support Washington, D.C. 20528 Telephone: (202) 447-5010

15.0 EMPLOYMENT ELIGIBILITY

The contractor will ensure that each employee working on this contract has a Social Security Card issued and approved by the Social Security Administration. The contractor will be responsible to the Government for acts and omissions of its own employees and for any sub-contractor(s) and their employees.

Subject to existing law, regulations and/ or other provisions of this contract, illegal or undocumented aliens will not be employed by the contractor, or with this contract. The contractor will ensure that this provision is expressly incorporated into any and all subcontracts or subordinate agreements issued in support of this contract.

16.0 CONTINUED ELIGIBILITY

DHS reserves the right and prerogative to deny and/ or restrict the facility and information access of any Contractor employee whom DHS determines to present a risk of compromising sensitive Government information to which he or she would have access under this contract.

The Contractor will report to the DHS Security Office any adverse information coming to its attention concerning employees working under this contract. Reports based on rumor or innuendo will not be made. The subsequent termination of an employee does not obviate the requirement of the Contractor to submit this report.

The report will include employee’s name, social security number, along with the adverse information being reported.

The Security Office may require drug screening for probable cause at any time and/or when the Contractor independently identifies, circumstances where probable cause exists.

The Security Office must be notified of all terminations/ resignations within 5 days of occurrence. The Contractor will return to the COR any expired DHS-issued identification cards and building passes, or those of terminated employees. If an identification card or building pass

is not available to be returned, a report must be submitted to the COR, referencing the pass or card number, name of individual to whom issued, the last known location and disposition of the pass or card.

17.0 SUITABILITY DETERMINATION

DHS will have and exercise full control over granting; denying, withholding or terminating unescorted government facility and/or sensitive Government information access for Contractor employees, based upon the results of a background investigation. DHS may, as it deems appropriate, authorize and make a favorable entry on duty (EOD) decision based on preliminary security checks. The favorable EOD decision is required before employees requiring access to sensitive information will be allowed to commence work prior to the completion of the full investigation. The granting of a favorable EOD decision will not be considered as assurance that a full employment suitability authorization will follow. The granting of a favorable EOD decision or a full employment suitability determination will in no way prevent, preclude, or bar DHS from the withdrawing or terminating access to facilities or information at any time during the term of the contract. No employee of the Contractor will be allowed unescorted access to a Government facility without a favorable EOD decision or suitability determination by the Security Office.

Contractor employees' not needing access to sensitive DHS information, or recurring access to DHS' facilities, will not be subject to security suitability screening.

Contractor employees awaiting an EOD decision may begin work on the contract provided they do not access sensitive Government information. Limited access to Government buildings is allowable prior to the EOD decision if a cleared Government employee escorts the Contractor. This limited access is to allow Contractors to attend briefings, meetings and begin work.

18.0 INFORMATION TECHNOLOGY SECURITY CLEARANCE

When sensitive government information is processed on Department telecommunications and automated information systems, the Contractor agrees to provide for the administrative control of sensitive data being processed and to adhere to the procedures governing such data as outlined in *DHS IT Security Program Publication DHS MD 4300.Pub.* Contractor personnel must have favorably adjudicated background investigations commensurate with the defined sensitivity level.

Contractors who fail to comply with Department security policy are subject to having their access to Department IT systems and facilities terminated, whether or not the failure results in criminal prosecution. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions under a variety of laws (e.g., Privacy Act).

19.0 SECURITY

References:

DHS Management Directive 140-01, "Information Technology Security Program

- DHS National Security Systems Policy Directive 4300A, (Version 13.1, July 25, 2017) and DHS 4300A Sensitive Systems Handbook (Version 12.0, November 15, 2015)
- DHS National Security Systems Policy Directive 4300B, Version 10.1, November 21, 2018' for NSS Collateral (Unclass, Secret or Top Secret Collateral).
- 'DHS Sensitive Compartmented Information (SCI) Systems 4300C Instruction Manual, Version 2.1, March 24, 2017' for TS SCI/C-LAN.

19.1 SAFEGUARDING OF SENSITIVE INFORMATION (MAR 2015)

(a) Applicability. This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as "Contractor"). The Contractor shall insert the substance of this clause in all subcontracts.

(b) Definitions. As used in this clause—

"Personally Identifiable Information (PII)" means information that can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, either alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-personally identifiable information can become personally identifiable information whenever additional information is made publicly available—in any medium and from any source—that, combined with other available information, could be used to identify an individual.
PII is a subset of sensitive information. Examples of PII include, but are not limited to: name, date of birth, mailing address, telephone number, Social Security number (SSN), email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), static Internet protocol addresses, biometric identifiers such as fingerprint, voiceprint, iris scan, photographic facial images, or any other unique identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual.

"Sensitive Information" is defined in HSAR clause 3052.204-71, Contractor Employee Access, as any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized undercriteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an

authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

(3) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

"Sensitive Information Incident" is an incident that includes the known, potential, or suspected exposure, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or unauthorized access or attempted access of any Government system, Contractor system, or sensitive information.

"Sensitive Personally Identifiable Information (SPII)" is a subset of PII, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements. Examples of such PII include: Social Security numbers (SSN), driver's license or state identification number, Alien Registration Numbers (A-number), financial account number, and biometric identifiers such as fingerprint, voiceprint, or iris scan. Additional examples include any groupings of information that contain an individual's name or other unique identifier plus one or more of the following elements:

(i) Truncated SSN (such as last 4 digits)
(ii) Date of birth (month, day, and year)
(iii) Citizenship or immigration status
(iv) Ethnic or religious affiliation
(v) Sexual orientation
(vi) Criminal History
(vii) Medical Information
(viii) System authentication information such as mother's maiden name, account passwords or personal identification numbers (PIN)

Other PII may be "sensitive" depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PII but is not sensitive.

(c) Authorities. The Contractor shall follow all current versions of Government policies and guidance accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors, or available upon request from the Contracting Officer, including but not limited to:

(1) DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified (for Official Use Only) Information
(2) DHS Sensitive Systems Policy Directive 4300A
(3) DHS 4300A Sensitive Systems Handbook and Attachments
(4) DHS Security Authorization Process Guide
(5) DHS Handbook for Safeguarding Sensitive Personally Identifiable Information
(6) DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program
(7) DHS Information Security Performance Plan (current fiscal year)
(8) DHS Privacy Incident Handling Guidance
(9) Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at http://csrc.nist.gov/groups/STM/cmvp/standards.html
(10) National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations accessible at http://csrc.nist.gov/publications/PubsSPs.html
(11) NIST Special Publication 800-88 Guidelines for Media Sanitization accessible at http://csrc.nist.gov/publications/PubsSPs.html

(d) Handling of Sensitive Information. Contractor compliance with this clause, as well as the policies and procedures described below, is required.
(1) Department of Homeland Security (DHS) policies and procedures on Contractor personnel security requirements are set forth in various Management Directives (MDs), Directives, and Instructions. MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information describes how Contractors must handle sensitive but unclassified information. DHS uses the term "FOR OFFICIAL USE ONLY" to identify sensitive but unclassified information that is not otherwise categorized by statute or regulation. Examples of sensitive information that are categorized by statute or regulation are PCII, SSI, etc. DHS Sensitive Systems Policy Direction 4300A Version 13.1, July 27, 2017 provide the policies and procedures on security for Information Technology (IT) resources. The DHS Handbook for Safeguarding Sensitive Personally Identifiable Information provides guidelines to help safeguard SPII in both paper and electronic form. DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program establishes procedures, program responsibilities, minimum standards, and reporting protocols for the DHS Personnel Suitability and Security Program.
(2) The Contractor shall not use or redistribute any sensitive information processed, stored, and/or transmitted by the Contractor except as specified in the contract.
(3) All Contractor employees with access to sensitive information shall execute DHS Form 11000-6, Department of Homeland Security Non-Disclosure Agreement (NDA), as a condition of access to such information. The Contractor shall maintain signed copies of the NDA for all employees as a record of compliance. The Contractor shall provide copies of the signed NDA to the Contracting Officer's Representative (COR) no later than two (2) days after execution of the form.

(4) The Contractor's invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions shall not maintain SPII. It is acceptable to maintain in these systems the names, titles and contact information for the COR or other Government personnel associated with the administration of the contract, as needed.

(e) Authority to Operate. The Contractor shall not input, store, process, output, and/or transmit sensitive information within a Contractor IT system without an Authority to Operate (ATO) signed by the Headquarters or Component CIO, or designee, in consultation with the Headquarters or Component Privacy Officer. Unless otherwise specified in the ATO letter, the ATO is valid for three (3) years. The Contractor shall adhere to current Government policies, procedures, and guidance for the Security Authorization (SA) process as defined below.

(i) Complete the Security Authorization process. The SA process shall proceed according to the DHS Sensitive Systems Policy Directive 4300A: (Version 13.1, July 27, 2017), or any successor publication, DHS 4300A Sensitive Systems Handbook (Version 12.0, November 15, 2015), or any successor publication, and the Security Authorization Process Guide including templates.

(ii) Security Authorization Process Documentation. SA documentation shall be developed using the Government provided Requirements Traceability Matrix and Government security documentation templates. SA documentation consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment Report, and Authorization to Operate Letter. Additional documents that may be required include a Plan(s) of Action and Milestones and Interconnection Security Agreement(s). During the development of SA documentation, the Contractor shall submit a signed SA package, validated by an independent third party, to the COR for acceptance by the Headquarters or Component CIO, or designee, at least thirty (30) days prior to the date of operation of the IT system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of a modified SA package. Once the ATO has been accepted by the Headquarters or Component CIO, or designee, the Contracting Officer shall incorporate the ATO into the contract as a compliance document. The Government's acceptance of the ATO does not alleviate the Contractor's responsibility to ensure the IT system controls are implemented and operating effectively.

(iii) Independent Assessment. Contractors shall have an independent third party validate the security and privacy controls in place for the system(s). The independent third party shall review and analyze the SA package, and report on technical, operational, and management level deficiencies as outlined in NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations. The Contractor shall address all deficiencies before submitting the SA package to the Government for acceptance.

(iv) Support the completion of the Privacy Threshold Analysis (PTA) as needed. As part of the SA process, the Contractor may be required to support the Government in the completion of the PTA. The requirement to complete a PTA is triggered by the

creation, use, modification, upgrade, or disposition of a Contractor IT system that will store, maintain and use PII, and must be renewed at least every three (3) years. Upon review of the PTA, the DHS Privacy Office determines whether a Privacy Impact Assessment (PIA) and/or Privacy Act System of Records Notice (SORN), or modifications thereto, are required. The Contractor shall provide all support necessary to assist the Department in completing the PIA in a timely manner and shall ensure that project management plans and schedules include time for the completion of the PTA, PIA, and SORN (to the extent required) as milestones. Support in this context includes responding timely to requests for information from the Government about the use, access, storage, and maintenance of PII on the Contractor's system, and providing timely review of relevant compliance documents for factual accuracy. Information on the DHS privacy compliance process, including PTAs, PIAs, and SORNs, is accessible at http://www.dhs.gov/privacy-compliance.

(2) Renewal of ATO. Unless otherwise specified in the ATO letter, the ATO shall be renewed every three (3) years. The Contractor is required to update its SA package as part of the ATO renewal process. The Contractor shall update its SA package by one of the following methods: (1) Updating the SA documentation in the DHS automated information assurance tool for acceptance by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls; or (2) Submitting an updated SA package directly to the COR for approval by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls. The 90 day review process is independent of the system production date and therefore it is important that the Contractor build the review into project schedules. The reviews may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place.

(3) Security Review. The Government may elect to conduct random periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS, the Office of the Inspector General, and other Government organizations access to the Contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The Contractor shall, through the Contracting Officer and COR, contact the Headquarters or Component CIO, or designee, to coordinate and participate in review and inspection activity by Government organizations external to the DHS. Access shall be provided, to the extent necessary as determined by the Government, for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of Government data or the function of computer systems used in performance of this contract and to preserve evidence of computer crime.

(4) Continuous Monitoring. All Contractor-operated systems that input, store, process, output, and/or transmit sensitive information shall meet or exceed the continuous monitoring requirements identified in the Fiscal Year 2014 DHS Information Security Performance Plan, or successor publication. The plan is updated on an annual basis. The Contractor shall also store monthly continuous monitoring data at its location for a period

not less than one year from the date the data is created. The data shall be encrypted in accordance with FIPS 140-2 Security Requirements for Cryptographic Modules and shall not be stored on systems that are shared with other commercial or Government entities. The Government may elect to perform continuous monitoring and IT security scanning of Contractor systems from Government tools and infrastructure.

(5) Revocation of ATO. In the event of a sensitive information incident, the Government may suspend or revoke an existing ATO (either in part or in whole). If an ATO is suspended or revoked in accordance with this provision, the Contracting Officer may direct the Contractor to take additional security measures to secure sensitive information. These measures may include restricting access to sensitive information on the Contractor IT system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls.

(6) Federal Reporting Requirements. Contractors operating information systems on behalf of the Government or operating systems containing sensitive information shall comply with Federal reporting requirements. Annual and quarterly data collection will be coordinated by the Government. Contractors shall provide the COR with requested information within three (3) business days of receipt of the request. Reporting requirements are determined by the Government and are defined in the Fiscal Year 2014 DHS Information Security Performance Plan, or successor publication. The Contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for Contractor systems.

(f) Sensitive Information Incident Reporting Requirements.

(1) All known or suspected sensitive information incidents shall be reported to the Headquarters or Component Security Operations Center (SOC) within one hour of discovery in accordance with 4300A Sensitive Systems Handbook Incident Response and Reporting requirements. When notifying the Headquarters or Component SOC, the Contractor shall also notify the Contracting Officer, COR, Headquarters or Component Privacy Officer, and US-CERT using the contact information identified in the contract. If the incident is reported by phone or the Contracting Officer's email address is not immediately available, the Contractor shall contact the Contracting Officer immediately after reporting the incident to the Headquarters or Component SOC. The Contractor shall not include any sensitive information in the subject or body of any e-mail. To transmit sensitive information, the Contractor shall use FIPS 140-2 Security Requirements for Cryptographic Modules compliant encryption methods to protect sensitive information in attachments to email. Passwords shall not be communicated in the same email as the attachment. A sensitive information incident shall not, by itself, be interpreted as evidence that the Contractor has failed to provide adequate information security safeguards for sensitive information, or has otherwise failed to meet the requirements of the contract.

(2) If a sensitive information incident involves PII or SPII, in addition to the reporting requirements in 4300A Sensitive Systems Handbook Incident Response and Reporting, Contractors shall also provide as many of the following data elements that are available at

the time the incident is reported, with any remaining data elements provided within 24 hours of submission of the initial incident report:

(i) Data Universal Numbering System (DUNS);

(ii) Contract numbers affected unless all contracts by the company are affected;

(iii) Facility CAGE code if the location of the event is different than the prime contractor location;

(iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, email);

(v) Contracting Officer POC (address, telephone, email);

(vi) Contract clearance level;

(vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;

(viii) Government programs, platforms or systems involved;

(ix) Location(s) of incident;

(x) Date and time the incident was discovered;

(xi) Server names where sensitive information resided at the time of the incident, both at the Contractor and subcontractor level;

(xii) Description of the Government PII and/or SPII contained within the system;

(xiii) Number of people potentially affected and the estimate or actual number of records exposed and/or contained within the system; and

(xiv) Any additional information relevant to the incident.

(g) Sensitive Information Incident Response Requirements.

(1) All determinations related to sensitive information incidents, including response activities, notifications to affected individuals and/or Federal agencies, and related services (e.g., credit monitoring) will be made in writing by the Contracting Officer in consultation with the Headquarters or Component CIO and Headquarters or Component Privacy Officer.

(2) The Contractor shall provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents.

(3) Incident response activities determined to be required by the Government may include, but are not limited to, the following:

(i) Inspections,

(ii) Investigations,

(iii) Forensic reviews, and

(iv) Data analyses and processing.

(4) The Government, at its sole discretion, may obtain the assistance from other Federal agencies and/or third-party firms to aid in incident response activities.

(h) Additional PII and/or SPII Notification Requirements.

(1) The Contractor shall have in place procedures and the capability to notify any individual whose PII resided in the Contractor IT system at the time of the sensitive information incident not later than 5 business days after being directed to notify individuals, unless otherwise approved by the Contracting Officer. The method and content of any

notification by the Contractor shall be coordinated with, and subject to prior written approval by the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, utilizing the DHS Privacy Incident Handling Guidance. The Contractor shall not proceed with notification unless the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, has determined in writing that notification is appropriate.

(2) Subject to Government analysis of the incident and the terms of its instructions to the Contractor regarding any resulting notification, the notification method may consist of letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by the Government. Notification may require the Contractor's use of address verification and/or address location services. At a minimum, the notification shall include:

(i) A brief description of the incident;
(ii) A description of the types of PII and SPII involved;
(iii) A statement as to whether the PII or SPII was encrypted or protected by other means;
(iv) Steps individuals may take to protect themselves;
(v) What the Contractor and/or the Government are doing to investigate the incident, to mitigate the incident, and to protect against any future incidents; and
(vi) Information identifying who individuals may contact for additional information.

(i) Credit Monitoring Requirements. In the event that a sensitive information incident involves PII or SPII, the Contractor may be required to, as directed by the Contracting Officer:

(1) Provide notification to affected individuals as described above; and/or

(2) Provide credit monitoring services to individuals whose data was under the control of the Contractor or resided in the Contractor IT system at the time of the sensitive information incident for a period beginning the date of the incident and extending not less than 18 months from the date the individual is notified. Credit monitoring services shall be provided from a company with which the Contractor has no affiliation. At a minimum, credit monitoring services shall include:

(i) Triple credit bureau monitoring;
(ii) Daily customer service;
(iii) Alerts provided to the individual for changes and fraud; and
(iv) Assistance to the individual with enrollment in the services and the use of fraud alerts; and/or

(3) Establish a dedicated call center. Call center services shall include:

(i) A dedicated telephone number to contact customer service within a fixed period;
(ii) Information necessary for registrants/enrollees to access credit reports and credit scores;
(iii) Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics;
(iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;
(v) Customized FAQs, approved in writing by the Contracting Officer in coordination with the Headquarters or Component Chief Privacy Officer; and

(vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

(j) Certification of Sanitization of Government and Government-Activity-Related Files and Information. As part of contract closeout, the Contractor shall submit the certification to the COR and the Contracting Officer following the template provided in NIST Special Publication 800-88 Guidelines for Media Sanitization.

19.2 INFORMATION SECURITY AND PRIVACY TRAINING (MAR 2015)

(a) Applicability. This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as "Contractor"). The Contractor shall insert the substance of this clause in all subcontracts.

(b) Security Training Requirements.

(1) All users of Federal information systems are required by Title 5, Code of Federal Regulations, Part 930.301, Subpart C, as amended, to be exposed to security awareness materials annually or whenever system security changes occur, or when the user's responsibilities change. The Department of Homeland Security (DHS) requires that Contractor employees take an annual Information Technology Security Awareness Training course before accessing sensitive information under the contract. Unless otherwise specified, the training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall complete the training before accessing sensitive information under the contract. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, initial training certificates for each Contractor and subcontractor employee shall be provided to the Contracting Officer's Representative (COR) not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

(2) The DHS Rules of Behavior apply to every DHS employee, Contractor and subcontractor that will have access to DHS systems and sensitive information. The DHS Rules of Behavior shall be signed before accessing DHS systems and sensitive information. The DHS Rules of Behavior is a document that informs users of their responsibilities when accessing DHS systems and holds users accountable for actions taken while accessing DHS systems and using DHS Information Technology resources capable of inputting, storing, processing, outputting, and/or transmitting sensitive information. The DHS Rules of Behavior is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Unless otherwise specified, the DHS Rules of Behavior shall be signed within thirty (30) days of contract award. Any new Contractor employees assigned to the contract shall also sign the DHS Rules of Behavior before accessing DHS systems and sensitive information. The Contractor shall maintain signed copies of the DHS Rules of Behavior for all Contractor and subcontractor employees as a record of compliance.

Unless otherwise specified, the Contractor shall e-mail copies of the signed DHS Rules of Behavior to the COR not later than thirty (30) days after contract award for each employee. The DHS Rules of Behavior will be reviewed annually and the COR will provide notification when a review is required.

(c) Privacy Training Requirements. All Contractor and subcontractor employees that will have access to Personally Identifiable Information (PII) and/or Sensitive PII (SPII) are required to take Privacy at DHS: Protecting Personal Information before accessing PII and/or SPII. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall also complete the training before accessing PII and/or SPII. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Initial training certificates for each Contractor and subcontractor employee shall be provided to the COR not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

20.0 ADVERTISING, PUBLICIZING AWARDS AND NEWS RELEASES

Under no circumstances shall the contractor, or anyone acting on behalf of the contractor, refer to the supplies, services, or equipment furnished pursuant to the provisions of this contract in any publicity/ news release or commercial advertising without first obtaining explicit written consent to do so from the COR and Contracting Officer.

This restriction does not apply to marketing materials developed for presentation to potential government customers of this contract vehicle.

The contractor agrees not to refer to awards in commercial advertising in such a manner as to state or imply that the product or service provided is endorsed or preferred by the Federal Government or is considered by the Government to be superior to other products or services.

The contractor shall not make any press/news releases pertaining to this procurement without prior Government approval and only in coordination with the GSA CO and DHS COR.

21.0 NON-PERSONAL SERVICES

The Government and the contractor understand and agree that the services delivered by the contractor to the Government are non-personal services. The parties also recognize and agree that no employer-employee or master-servant relationship exists or will exist between the Government and the contractor. The contractor and the contractor's employees are not employees of the Federal Government and are not eligible for entitlement and benefits given federal employees.

Contractor personnel under this task order shall not (i) be placed in a position where there is an appearance that they are employed by a Federal Officer, or are under the supervision, direction,

or evaluation of a Federal Officer, or (ii) be placed in a position of command, supervision, administration, or control over Government personnel.

22.0 CONTRACTOR PERSONNEL

The contractor shall ensure that its staff and subcontractors maintain any generally required professional certifications, accreditations, and proficiency relative to their areas of expertise. The contractor shall retain documentation of such records. The Government will not pay expenses to meet this requirement.

22.1 IDENTIFICATION OF CONTRACTOR PERSONNEL

The contractor shall ensure that its employees will identify themselves as employees of their respective company while working on CISA/GSA contracts. For example, contractor personnel shall introduce themselves in person, voicemail, email and sign attendance logs as employees of their respective companies, and not as CISA employees. The contractor shall ensure that their personnel use the following format signature on all official e-mails generated by CISA computers:

Name

Position or Professional Title Company Name

Supporting the CISA/IP/SOPD/Office of DHS Phone

Other contact information as desired.

23.0 PRINTING RESTRICTIONS

All printing funded by this task order must be done in conformance with Joint Committee on Printing regulations as prescribed in Title 44, United States Code, and Section 308 of Public Law 101-163, and all applicable Government Printing Office and Department of Homeland Security regulations.

24.0 EMPLOYEE IDENTIFICATION

Contractor employees visiting Government facilities shall wear an identification badge that, at a minimum, displays the contractor name, the employee's photo, name, clearance-level and badge expiration date. Visiting contractor employees shall comply with all Government escort rules and requirements. All contractor employees shall identify themselves as contractors when their status is not readily apparent and display all identification and visitor badges in plain view above the waist at all times.

Government issued identification badge. All contractor employees shall identify themselves as contractors when their status is not readily apparent (in meetings, when answering Government telephones, in e-mail messages, etc.) and display the Government issued badge in plain view above the waist at all times.

25.0 EMPLOYEE CONDUCT

Contractor's employees shall comply with all applicable Government regulations, policies and procedures (e.g., fire, safety, sanitation, environmental protection, security, "off limits" areas) when visiting or working at government facilities. The contractor shall ensure contractor employees present a professional appearance at all times and that their conduct shall not reflect discredit on the United States or the Department of Homeland Security. The contractor shall ensure its employees understand and abide by Department of Homeland Security established rules, regulations and policies concerning safety and security.

25.1 REMOVING EMPLOYEES FOR MISCONDUCT OR SECURITY REASONS

The Government may, at its sole discretion (via the Contracting Officer), direct the contractor to remove any contractor employee from DHS facilities for misconduct or security reasons. Removal does not relieve the contractor of the responsibility to continue providing the services required under this task order. The Contracting Officer will provide the contractor with a written explanation to support any request to remove an employee.

26.0 CONTRACTOR PERSONNEL

26.1 NOTIONAL STAFFING REFERENCE

Attachment X represents notional level of effort, based on historical and forecasted contract support that may be needed for this TO. The contractor shall utilize the Attachment as a reference, but shall propose a labor mix or level of effort in support of their solution to meeting the TO requirements that may or may not be in accordance with the attachment.

26.2 QUALIFIED PERSONNEL

The contractor shall provide qualified personnel to perform all requirements specified in this PWS.

26.3 CONTINUITY OF SUPPORT

The contractor shall ensure that the contractually required level of support for this requirement is maintained at all times. The contractor shall ensure that all contract support personnel are present for all hours of the workday. If for any reason the contractor staffing levels are not maintained due to vacation, leave, appointments, etc., and replacement personnel will not be provided, the Contractor shall provide email notification to the CO, CS and the COR at least one week prior to employee absence. Otherwise, the contractor shall provide a fully qualified replacement.

26.4 KEY PERSONNEL

Before replacing any individual designated as *Key* by the Government, the contractor shall notify the Contracting Officer no less than 15 business days in advance, submit written justification for replacement, and provide the name and qualifications of any proposed substitute(s). All proposed substitutes shall possess qualifications equal to or superior to those of the *Key* person being replaced unless otherwise approved by the Contracting Officer. The Contractor shall not remove

or replace *Key* contractor personnel without prior approval from the Contracting Officer. The following contractor personnel are designated as Key for this requirement.

The following are the minimum personnel who shall be designated as "Key." The Government does not intend to dictate the composition of the ideal team to perform this TO. The Government will evaluate up to three additional Key Personnel as proposed by the contractor.

The key personnel for this TO shall be:

26.4.1 PROGRAM MANAGER

The contractor shall identify a PM to serve as the Government's main POC and to provide overall leadership and guidance for all contractor personnel assigned to the TO. The PM shall ultimately be responsible for the quality and efficiency of the TO. The PM shall have organizational authority to execute the requirements of the TO. The PM shall assign tasking to contractor personnel, supervise ongoing technical efforts, and manage overall TO performance to ensure the optimal use of assigned resources and subcontractors. This Key Person shall have the ultimate authority to commit the contractor's organization and make decisions for the contractor's organization in response to Government issues, concerns, or problems. The PM shall be readily available to respond to Government questions, concerns, and comments, as well as be proactive in alerting the Government to potential contractual and programmatic issues.

The PM shall possess all required qualifications (below) at time of proposal submission:

a. Employee of the prime contractor.
b. Possess current Top Secret Clearance.
c. At least eight years of experience managing and supervising staff and leading multi-disciplinary teams on performance-based projects similar to the TO scope.
d. At least eight years of experience in completing, leading, or directing the work of others on projects similar to the size, scope, and complexity of the work and environment described above.
e. Managerial experience providing technical advice, organizing, planning, directing, and managing staff to ensure goals and objectives are achieved.
f. Experience with risk management, issue resolution, problem solving, and customer service.
g. Current Project Management Institute (PMI) Project Management Professional, Program Management Professional certification, MBA, or equivalent.

26.4.2 DEPUTY PROGRAM MANAGER

The contractor shall identify a DPM to serve as the Government's alternate POC. Performance of work requires a mastery of a wide range of management concepts, principles, methods, techniques and practices to manage all facets of the scope of the TO. The DPM responsibilities shall include day-to-day functioning of all activities, providing effective management and direction for the TO.

The DPM shall possess all required qualifications (below) at time of proposal submission:

a. Employee of the prime contractor.
b. Possess current active Top Secret Clearance.
c. At least five years of experience managing, supervising, or being a team lead for multi-disciplinary teams on performance-based projects.
d. Managerial experience providing technical advice, organizing, planning, directing, and managing staff to ensure goals and objectives are achieved.
e. Experience with risk management, issue resolution, problem solving, and customer service.
f. Current Project Management Institute (PMI) Project Management Professional, Program Management Professional certification, MBA, or equivalent.

26.4.3 KEY PERSONNEL SUBSTITUTION

The contractor shall not replace any personnel designated as Key Personnel without the written concurrence of the GSA CO. Prior to using other than personnel specified in proposals in response to a TO, the contractor shall notify the GSA CO and the COR. This notification shall be NLT ten calendar days in advance of any proposed substitution and shall include justification (including resume(s), and labor category of proposed substitution(s)) in sufficient detail to permit evaluation of the impact on TO performance.

Substitute personnel qualifications shall be equal to, or greater than, those of the person being substituted. If the GSA CO and thec COR determine that a proposed substitute person is unacceptable, or that the reduction of effort would be so substantial as to impair the successful performance of the work under the TO, the contractor may be subject to default action as prescribed by FAR 52.249-6, Termination (Cost-Reimbursement).

In the event of key personnel departures, the contractor shall ensure support for all CISA requirements until permanent replacements are available. The contractor shall identify a qualified successor candidate on an acting or permanent basis, within 30 business days after the departure of a key individual; final approval of key personnel is the responsibility of CISA.

27.0 PRIVACY

The contractor shall provide training for all employees and subcontractors that have access to Sensitive Personally Identifiable Information (SPII) as well as the creation, use, dissemination and / or destruction of SPII, at the outset of the subcontractor's /employee's work on the and every year thereafter. Said training would include procedures on how to properly handle SPII, to include security requirements for transporting or transmitting SPII information, requirements for reporting a suspected breach or loss of SPII within one hour and supporting privacy compliance and breach management activities. The Contractor must submit an e-mail notification to the CISA COR that all the Contractor's employees have received privacy training prior to the beginning of the task order.

The Federal Information Security Management Act (FISMA) requires all individuals accessing CISA information, regardless of their employment status, be they Federal or contractor employees, to take the annual Information Security and Records Management Training annually.

Both courses (Information Security and Records Management) can be obtained via Government-provided CD. The Contractor shall maintain copies of certificates as a record of compliance. The Contractor shall submit an annual e-mail notification to the CISA COR that the required Information Security, Records Management, and Privacy training has been completed for all of the Contractor's employees.

The privacy training can be obtained via Government-provided CD or through the Homeland Security Information Network (HSIN) at https://share.dhs.gov/nppdprivacy101training/. DHS has also published a guidebook defining SPII and setting standards for SPII handling and protection. The DHS Handbook for Safeguarding SPII is a 30-page public document on the DHS Privacy Office website.

Link:http://www.dhs.gov/sites/default/files/publications/privacy/Guidance/handbookforsafeguardingse nsitivePII_march_2012_webversion.pdf

28.0 ACCOUNTABLE PROPERTY

Definitions:

- Accountable Personal Property - An asset that meets one or more of the following criteria: (1) expected useful life is two years or longer and an asset value and/or acquisition cost of $5,000 or more; (2) that is classified as sensitive; (3) for which accountability or property control records are maintained; (4) Capitalized personal property, (5) Leased property that meets accountability standards, or (6) otherwise warrants tracking in the property system of record. Current accountable personal property information may be obtained through the CSD APO Office at cs&cassetmanagementteam@hq.dhs.gov.
- Capitalized Personal Property - Non-expendable personal property with an acquisition cost over an established threshold and a normal life expectancy of two years or more. Current Capitalization Threshold information may be obtained through the CSD APO Office at cs&cassetmanagementteam@hq.dhs.gov.
- Contract Property - Contract property refers to both Contractor-Acquired Property (CAP) and GFP, in the possession of contractors.
- Contractor Acquired Property (CAP) - Property acquired, fabricated, or otherwise provided by the contractor for performing a contract and to which the Government has title.
- Government Furnished Property (GFP) - Property in the possession of, or directly acquired by, the Government and subsequently furnished to the contractor for performance of a contract. Government-furnished property includes, but is not limited to, spares and property furnished for repair, maintenance, overhaul, or modification. Government-furnished property also includes contractor-acquired property if the contractor-acquired property is a deliverable under a cost contract when accepted by the Government for continued use under the contract. NOTE: GFP may also be referred to as Government Furnished Equipment (GFE), the two terms are interchangeable.

- Leased Property - Property that is not owned by DHS, but that is leased by the Government under terms as stipulated in the lease agreement (this excludes the leasing of property by contractors in the performance of a contract).
- Sensitive Personal Property - All items, regardless of value, that require special control and accountability due to unusual rates of loss, theft, or misuse; national security or export control considerations. Such property includes but is not limited to, weapons, ammunition, explosives, information technology equipment with memory capability, cameras, and communications equipment. Current sensitive personal property information may be obtained through the CSD APO Office at cs&cassetmanagementteam@hq.dhs.gov.

Property Accountability:

- When contractors are furnished with GFP, DHS barcodes will not be removed. In all GFP cases, the Government retains title to the property
- It is the contractor's responsibility to use contract property as it was authorized, and for the purpose intended. In the event the contractor uses contract property for other purposes without written authorization from the CO, the contractor may be liable for rental, without credit, of such items for each month or part of a month in which such unauthorized use occurs
- Contractor is directly responsible and accountable for all contract property in its possession in accordance with the requirements of the particular contract; this also includes any contract property in the possession or control of a subcontractor

Physical inventory: In addition to requirements provided under the contract's government property clause:

- The Contractor shall, minimum annually, perform, record, and disclose physical inventory results of CAP and GFP to the CSD APO Office at cs&cassetmanagementteam@hq.dhs.gov, PA and/or COR
- Annual inventory results will be completed, certified and submitted by close of business 31 May each year to the CSD APO Office at cs&cassetmanagementteam@hq.dhs.gov, PA and/or COR
- The Contractor shall, upon request, perform, record, and disclose physical inventory results of CAP and GFP to the CSD APO Office cs&cassetmanagementteam@hq.dhs.gov., PA and/or COR
- As requested inventory results will be completed, certified and submitted, in the timeframe defined at the time of request, to the CSD APO Office at cs&cassetmanagementteam@hq.dhs.gov., PA and/or COR

Property Disposal:

- All documentation and goods are the property of the United States Government and, if applicable, the contractor shall return or destroy appropriately upon request. The contractor shall comply with applicable government rules and regulations for disposal of government property. Further, the contractor shall provide necessary information to the PA, COR and the CSD APO Office at cs&cassetmanagementteam@hq.dhs.gov. For

all excess property prior to taking any action. Excess personal property" means any personal property under the control of a Federal agency that the agency head determines is not required for its needs or for the discharge of its responsibilities.

Lost, Stolen, Damaged or Destroyed (LDD) property:

- Unless otherwise provided in the contract, the contractor is liable for LDD of contract property, except for reasonable wear and tear in accordance with the contract's government property clause.
- Any occurrence of LDD must be investigated and fully documented by the PA and/or COR, who will promptly notify the CO. The contractor will submit a report of any incident of LDD contract property to the PA in accordance with the contract's government property clause and as detailed below, as soon as it becomes known
- When GFP or CAP property is LDD, the Contractor must report within 24 hours of discovery of the event to the COR who will initiate a Report of Survey. This document will be obtained from CSD APO Office at cs&cassetmanagementteam@hq.dhs.gov.
- A Report of Survey will be prepared, regardless whether or not preliminary research of a LDD event indicates positive evidence of negligence, misconduct, or unauthorized use and the responsible individual refuses to admit pecuniary liability.
- The Contractor must forward this document with all supporting documentation to the PA or COR within 5 business days of the LDD event for review.
- The PA and/or COR must submit the completed package to cs&cassetmanagementteam@hq.dhs.gov.within 5 business days of receipt from the Contractor.
- Contractor, PA and/or COR must supply all requested information and any subsequent requests for information.

29.0 SECTION 508 COMPLIANCE

29.1 SECTION 508 REQUIREMENTS

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) (codified at 29 U.S.C. § 794d) requires that when Federal agencies develop, procure, maintain, or use information and communications technology (ICT), it shall be accessible to people with disabilities. Federal employees and members of the public with disabilities must be afforded access to and use of information and data comparable to that of Federal employees and members of the public without disabilities.

1. All products, platforms and services delivered as part of this work statement that, by definition, are deemed ICT or that contain ICT shall conform to the revised regulatory implementation of Section 508 Standards, which are located at 36 C.F.R. § 1194.1 & Apps. A, C & D, and available at: https://www.gpo.gov/fdsys/pkg/CFR-2017-title36-vol3/pdf/CFR-2017-title36-vol3- part1194.pdf. In the revised regulation, ICT replaced the term electronic and information technology (EIT) used in the original 508 standards.

2. When providing installation, configuration or integration services for ICT, the contractor shall not reduce the original ICT item's level of Section 508 conformance prior to the services being performed.
3. When providing maintenance upgrades, substitutions, and replacements to ICT, the contractor shall not reduce the original ICT's level of Section 508 conformance prior to upgrade, substitution or replacement. The agency reserves the right to request an Accessibility Conformance Report (ACR) for proposed substitutions and replacements prior to acceptance.

The ACR should be created using the on the Voluntary Product Accessibility Template Version 2.2 508 (or later). The template can be located at https://www.itic.org/policy/accessibility/vpat

1. When developing or modifying ICT for the government, the contractor shall ensure the ICT fully conforms to the applicable Section 508 Standards. When modifying a commercially available or government-owned ICT, the contractor shall not reduce the original ICT Item's level of Section 508 conformance.
2. When developing or modifying ICT that are delivered in an electronic Microsoft Office or Adobe PDF format, the contractor shall demonstrate conformance by providing Section 508 test results based on the Accessible Electronic Documents – Community of Practice (AED COP) Harmonized Testing Guidance at https://www.dhs.gov/508-testing.
3. When developing or modifying software that generates electronic content (e.g., an authoring tool that is used to create html pages, reports, surveys, charts, dashboards, etc.), the contractor shall ensure software can be used to create electronic content that conforms to the Section 508 standards.
4. Contractor personnel shall possess the knowledge, skills and abilities necessary to address the applicable revised Section 508 Standards for each ICT.
5. Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the Contracting Officer and a determination will be made according to DHS Directive 139-05, Office of Accessible Systems and Technology, dated November 12, 2018 and DHS Instruction 139-05-001, Managing the Accessible Systems and Technology Program, dated November 20, 2018.

29.1.1 INSTRUCTIONS TO OFFERORS

1. For each ICT Item that will be developed, modified, installed, configured, integrated, maintained, or hosted by the contractor pursuant to this contract, the offeror shall provide an acknowledgement of the Section 508 requirements and a detailed explanation of the Offerors plan to ensure conformance with the requirements. The Offeror shall also describe the evaluation methods that will be used to validate for conformance to the Section 508 Standards.
2. The offeror shall describe plans for features that do not fully conform to the Section 508 Standards.

29.1.2 ACCEPTANCE CRITERIA

Before accepting items that contain Information and Communications Technology (ICT) that are developed, modified, or configured according to this contract, the government reserves the right to require the contractor to provide the following:

1. Accessibility test results based on the required test methods.
2. Documentation of features provided to help achieve accessibility and usability for people with disabilities.
3. Documentation of core functions that cannot be accessed by persons with disabilities.
4. Documentation on how to configure and install the ICT Item to support accessibility.
5. Demonstration of the ICT Item's conformance to the applicable Section 508 Standards, (including the ability of the ICT Item to create electronic content – where applicable).
6. Before accepting ICT required under the contract, the government reserves the right to perform testing on required ICT items to validate the offeror's Section 508 conformance claims. If the government determines that Section 508 conformance claims provided by the offeror represent a higher level of conformance than what is actually provided to the agency, the government shall, at its option, require the offeror to remediate the item to align with the offeror's original Section 508 conformance claims prior to acceptance.